PHYSICAL REVIEW A **95**, 010101(R) (2017)

Multipartite Gaussian steering: Monogamy constraints and quantum cryptography applications

Yu Xiang,[1,2,*] Ioannis Kogias,[3,†] Gerardo Adesso,[3,‡] and Qiongyi He[1,2,§]

[1]*State Key Laboratory of Mesoscopic Physics, School of Physics, Peking University, Collaborative Innovation Center of Quantum Matter, Beijing 100871, China*

[2]*Collaborative Innovation Center of Extreme Optics, Shanxi University, Taiyuan, Shanxi 030006, China*

[3]*School of Mathematical Sciences, University of Nottingham, Nottingham NG7 2RD, United Kingdom*

(Received 31 March 2016; revised manuscript received 27 June 2016; published 12 January 2017)

We derive laws for the distribution of quantum steering among different parties in multipartite Gaussian states under Gaussian measurements. We prove that a monogamy relation akin to the generalized Coffman-Kundu-Wootters inequality holds quantitatively for a recently introduced measure of Gaussian steering. We then define the residual Gaussian steering, stemming from the monogamy inequality, as an indicator of collective steering-type correlations. For pure three-mode Gaussian states, the residual acts as a quantifier of genuine multipartite steering, and is interpreted operationally in terms of the guaranteed key rate in the task of secure quantum secret sharing. Optimal resource states for the latter protocol are identified, and their possible experimental implementation discussed. Our results pin down the role of multipartite steering for quantum communication.

DOI: 10.1103/PhysRevA.95.010101

With the imminent debacle of Moore's law, and the constant need for faster and more reliable processing of information, quantum technologies are set to radically change the landscape of modern communication and computation. A successful and secure quantum network relies on quantum correlations distributed and shared over many sites [1]. Different kinds of multipartite quantum correlations have been considered as valuable resources for various applications in quantum communication tasks. Multipartite entanglement [2–8] and multipartite Bell nonlocality [9–12] are two well known instances and have received extensive attention in recent developments of quantum information theory, as well as in other branches of modern physics. There has been substantial experimental progress in the engineering and detection of both such correlations, by using, e.g., photons [13–17], ions [18], or continuous variable (CV) systems [19–22]. However, as an intermediate type of quantum correlation between entanglement and Bell nonlocality, multipartite quantum steering [23,24] still defies a complete understanding. In consideration of the intrinsic relevance of the notion of steering to the foundational core of quantum mechanics, it has become a worthwhile objective to deeply explore the characteristics of multipartite steering distributed over many parties, and to establish what usefulness to multiuser quantum communication protocols can such a resource provide, where bare entanglement is not enough and Bell nonlocality may not be accessible.

The concept of quantum steering was originally introduced by Schrödinger [25] to describe the "spooky action-at-a-distance" effect noted in the Einstein-Podolsky-Rosen (EPR) paradox [26–28], whereby local measurements performed on one party apparently adjust (steer) the state of another distant party. Recently identified as a distinct type of nonlocality [29,30], quantum steering is thus a directional form of quantum correlations, characterized by its inherent asymmetry between the parties [31–37]. Additionally, steering allows verification of entanglement, without assumptions of the full trust of reliability of equipment at all of the nodes of a communication network [38]. Steering is then a natural resource for one-sided device-independent quantum key distribution [39,40]. For bipartite systems, a comprehensive quantitative investigation of quantum steering has been recently proposed [41–44] and tested in several systems [45–51]. Comparatively little is known about steering in multipartite scenarios. For instance, Refs. [52–54] derived criteria to detect genuine multipartite steering, and Ref. [55] presented some limitations on joint quantum steering in tripartite systems.

In this Rapid Communication we focus on steerability of multipartite Gaussian states of CV systems by Gaussian measurements, a physical scenario which closely aligns with the traditional EPR paradox, and which is of primary relevance for experimental implementations [56–58]. In order to investigate the shareability of Gaussian steering from a quantitative perspective [36], we establish *monogamy* relations imposing constraints on the degree of bipartite EPR steering that can be shared among N-mode CV systems in pure Gaussian states, in analogy with the Coffman-Kundu-Wootters (CKW) monogamy inequality for entanglement [6,7,59–63]. We further propose an indicator of collective steering-type correlations, the *residual Gaussian steering* (RGS), stemming from the laws of steering monogamy, that is shown to act as a quantifier of genuine multipartite steering for pure three-mode Gaussian states. Finally, we show how the RGS acquires an operational interpretation in the context of a partially device-independent quantum secret sharing (QSS) protocol [64–68]. Specifically, taking into account arbitrary eavesdropping and potential cheating strategies of some of the parties [66], the achievable key rate of the protocol is shown to admit tight lower and upper bounds which are simple linear functions of the RGS. This in turn allows us to characterize optimal resources for CV QSS in terms of their multipartite steering.

(a) Monogamy of Gaussian steering. A fundamental property of entanglement, which has profound applications in

*xiangy.phy@pku.edu.cn
†john_k_423@yahoo.gr
‡gerardo.adesso@nottingham.ac.uk
§qiongyihe@pku.edu.cn

quantum communication, is known as monogamy [59,63,69]. Any two quantum systems that are maximally entangled with each other, cannot be entangled (or even classically correlated) with any other third system. Therefore, entanglement cannot be freely shared among different parties. In their seminal paper [59], CKW derived a monogamy inequality that quantitatively describes this phenomenon for any finite entanglement shared among arbitrary three-qubit states ρ: $\mathcal{C}^2_{A:(BC)}(\rho) \geqslant \mathcal{C}^2_{A:B}(\rho) + \mathcal{C}^2_{A:C}(\rho)$, where $\mathcal{C}^2_{A:(BC)}(\rho)$ is the squared concurrence, quantifying the amount of bipartite entanglement across the bipartition $A:(BC)$. Osborne and Verstraete later generalized the CKW monogamy inequality to n qubits [61]. For CV systems, however, both the quantification and the study of the distribution of entanglement constitute in general a considerably harder problem. Remarkably, if one focuses on the theoretically and practically relevant class of Gaussian states, various results similar to the qubit case have been derived, using different entanglement measures [6,7,56,60,62,70]. Of particular interest to us will be the fact that the Gaussian Rényi-2 entanglement monotone $\mathcal{E}_{A:B}(\rho_{AB})$, which quantifies entanglement of bipartite Gaussian states ρ_{AB}, has been shown to obey a CKW-type monogamy inequality for all m-mode Gaussian states $\rho_{A_1\ldots A_m}$ with covariance matrix (CM) $\sigma_{A_1\ldots A_m}$ [62],

$$\mathcal{E}_{A_k:(A_1,\ldots,A_{k-1},A_{k+1},\ldots,A_m)}\left(\sigma_{A_1\ldots A_m}\right) - \sum_{j\neq k} \mathcal{E}_{A_k:A_j}\left(\sigma_{A_1\ldots A_m}\right) \geqslant 0, \tag{1}$$

where each A_j comprises one mode only. Recall that the $2m \times 2m$ CM $\sigma_{A_1\ldots A_m}$ of a m-mode state $\rho_{A_1\ldots A_m}$ has elements $\sigma_{ij} = \mathrm{tr}[\{\hat{R}_i, \hat{R}_j\}_+ \rho]$, where $\hat{R} = (\hat{x}_1, \hat{p}_1, \ldots, \hat{x}_m, \hat{p}_m)^{\mathsf{T}}$ is the vector collecting position and momentum operators of each mode, satisfying canonical commutation relations $[\hat{R}_i, \hat{R}_j] = i(\Omega_{A_1\ldots A_m})_{ij}$, with $(\Omega_{A_1\ldots A_m}) = \omega^{\oplus m}$ and $\omega = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ being the single-mode symplectic form [56].

Quantum steering is a type of correlation that allows for entanglement certification in a multimode bipartite state ρ_{AB} even when one of the parties' devices, say Bob's, are completely uncharacterized (untrusted). In this case, we say that Bob can steer Alice's local state [29,30]. Keeping our focus on Gaussian states and measurements [36], the question, thus, naturally arises: is steering monogamous? Intuitively one would expect that there should exist limitations on the distribution of steering-type correlations, since steering is only a stronger form of the already monogamous entanglement. A first answer to this question was recently given by Reid [55], who showed that, under restrictions to measurements and detection criteria involving up to second order moments, if a single-mode party A can be steered by a single-mode party B then no other single-mode party C can simultaneously steer A. This was recently generalized to the case of parties B and C comprising an arbitrary number of modes [71,72]. Reference [55] also discussed other monogamy relations for steering and nonlocality both in discrete and CV systems.

In the following we provide general quantitative CKW-type limitations to the distribution of Gaussian steering among many parties. For our purposes, we will focus on a recently proposed Gaussian steering measure [36], $\mathcal{G}^{B\to A}(\sigma_{AB})$, which quantifies how much party B can steer party A in a Gaussian state with CM σ_{AB} by Gaussian measurements. In particular, we now show that the Gaussian steering measure $\mathcal{G}$ is monogamous, and hence satisfies a CKW-type monogamy inequality in direct analogy with entanglement. Consider an arbitrary (pure or mixed) m-mode Gaussian state $\rho_{A_1\ldots A_m}$ with CM $\sigma_{A_1\ldots A_m}$, where each party A_j comprises a single mode ($n_j = 1$, $\forall j = 1,\ldots,m$). Then, the following inequalities hold, $\forall\, k = 1,\ldots,m$:

$$\mathcal{G}^{(A_1,\ldots,A_{k-1},A_{k+1},\ldots,A_m)\to A_k}(\sigma_{A_1\ldots A_m}) - \sum_{j\neq k} \mathcal{G}^{A_j\to A_k}(\sigma_{A_1\ldots A_m}) \geqslant 0, \tag{2}$$

$$\mathcal{G}^{A_k\to(A_1,\ldots,A_{k-1},A_{k+1},\ldots,A_m)}(\sigma_{A_1\ldots A_m}) - \sum_{j\neq k} \mathcal{G}^{A_k\to A_j}(\sigma_{A_1\ldots A_m}) \geqslant 0. \tag{3}$$

For pure states with CM $\sigma^{\mathrm{pure}}_{A_1\ldots A_m}$, the proof is straightforward. Namely, recall from [36] that the first terms of (2), (3), and (1) all coincide on pure states. On the other hand, for the marginal states of any two modes i and j one has $\mathcal{E}_{A_i:A_j}(\sigma^{\mathrm{pure}}_{A_1\ldots A_m}) \geqslant \mathcal{G}^{A_i\to A_j}(\sigma^{\mathrm{pure}}_{A_1\ldots A_m})$ [36]. Inequalities (2) and (3) then follow readily from the monogamy inequality (1) for Gaussian entanglement. The full proof of the above inequalities for general mixed states is deferred to the Appendix.

The monogamy relations just derived in this work impose fundamental restrictions to the distribution of Gaussian steering among multiple parties in fully quantitative terms. To analyze these in more detail, let us focus on a tripartite scenario, in which the monogamy inequalities take the simpler form,

$$\mathcal{G}^{(AB)\to C}(\sigma_{ABC}) - \mathcal{G}^{A\to C}(\sigma_{ABC}) - \mathcal{G}^{B\to C}(\sigma_{ABC}) \geqslant 0, \tag{4}$$

$$\mathcal{G}^{C\to(AB)}(\sigma_{ABC}) - \mathcal{G}^{C\to A}(\sigma_{ABC}) - \mathcal{G}^{C\to B}(\sigma_{ABC}) \geqslant 0. \tag{5}$$

As in the original CKW inequality, these inequalities enjoy a very appealing interpretation: the degree of steering (by Gaussian measurements) exhibited by the state when all three parties are considered (i.e., $\mathcal{G}^{(AB)\to C} > 0$, or $\mathcal{G}^{C\to(AB)} > 0$) can be larger than the sum of the degrees of steering exhibited by the individual pairs. On a more extreme level, there exist quantum states where parties A and B cannot individually steer party C, i.e., $\mathcal{G}^{A\to C} = \mathcal{G}^{B\to C} = 0$, but collectively they can, i.e., $\mathcal{G}^{(AB)\to C} > 0$. We will see the importance of this type of correlations later when we discuss applications to QSS. We remark that the monogamy inequality (4) realizes a crucial nontrivial strengthening of Result 5 in [55], which can be recast as $\mathcal{G}^{(AB)\to C}(\sigma_{ABC}) - \frac{1}{2}\mathcal{G}^{A\to C}(\sigma_{ABC}) - \frac{1}{2}\mathcal{G}^{B\to C}(\sigma_{ABC}) \geqslant 0$ in our notation. On the other hand, the reverse monogamy relation (3) settles an open question raised in the same work [55].

The residuals of the subtractions in (4) and (5) quantify steering-type correlations that correspond to a collective property of the three parties, not reducible to the properties of the individual pairs. We proceed by investigating this quantitatively in a mode-invariant way. In analogy with what is done for entanglement [6,7,62], we can calculate the residuals from the monogamy inequalities (4) or (5) and minimize them over all mode permutations. It turns out that, in the paradigmatic case of pure three-mode Gaussian states with CM $\sigma^{\mathrm{pure}}_{ABC}$ ($m = 3$), we obtain the same quantity (RGS) from

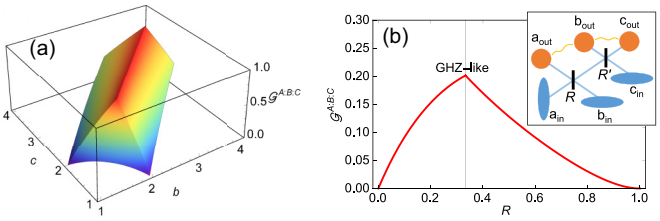

FIG. 1. Residual tripartite Gaussian steering $\mathcal{G}^{A:B:C}$ for pure three-mode Gaussian states with CM $\sigma^{\text{pure}}_{ABC}$ (a) with fixed $a = 2$ (local variance of subsystem A), and (b) generated by three squeezed vacuum fields at -3 dB injected in two beamsplitters with reflectivities R and R' (see inset), setting $R' = 1/2$ to obtain $b = c$; the permutationally invariant GHZ-like state ($a = b = c$) is obtained at $R = 1/3$.

either (4) or (5), regardless of the steering direction. Explicitly, denoting by $\langle i,j,k\rangle$ any cyclic permutation of A,B,C, the RGS for three-mode pure Gaussian states with CM $\sigma^{\text{pure}}_{ABC}$ is defined as

$$\mathcal{G}^{A:B:C}\left(\sigma^{\text{pure}}_{ABC}\right) = \min_{\langle i,j,k\rangle}\{\mathcal{G}^{(jk)\to i} - \mathcal{G}^{j\to i} - \mathcal{G}^{k\to i}\} \quad (6a)$$

$$= \min_{\langle i,j,k\rangle}\{\mathcal{G}^{i\to(jk)} - \mathcal{G}^{i\to j} - \mathcal{G}^{i\to k}\} \quad (6b)$$

$$= \ln[\min\{bc/a, ca/b, ab/c\}], \quad (6c)$$

where $a = \sqrt{\det\sigma_A}$, $b = \sqrt{\det\sigma_B}$, and $c = \sqrt{\det\sigma_C}$ are local symplectic invariants (with $|b-c|+1 \leqslant a \leqslant b+c-1$), fully determining the CM $\sigma^{\text{pure}}_{ABC}$ in standard form [7,62].

The RGS $\mathcal{G}^{A:B:C}$ is a monotone under Gaussian local operations and classical communication, as one can prove analogously to the case of the residual entanglement of Gaussian states [6,7,36,42,62]. Furthermore, finding a nonzero value of the RGS certifies genuine tripartite steering, as defined by He and Reid [52], since a sufficient requirement to violate the corresponding biseparable model for pure states is the demonstration of steering in all directions: $(BC) \to A$, $(AC) \to B$, and $(AB) \to C$. We can then regard the RGS as a meaningful quantitative indicator of genuine tripartite steering for pure three-mode Gaussian states under Gaussian measurements.

In Fig. 1(a) we plot the RGS as a function of b and c for a given a. An elementary analysis reveals that the RGS $\mathcal{G}^{A:B:C}$ is maximized on bisymmetric states with $b = c \geqslant a$, i.e., when the states are steerable across any global split of the three modes and also $B \leftrightarrow C$ steerable, but no other steering exists between any two parties. In this case, the genuine tripartite steering $\mathcal{G}^{A:B:C}$ reduces to the collective steering $\mathcal{G}^{(BC)\to A} = \mathcal{G}^{A\to(BC)} = \ln a$. This quantitative analysis completes the existing picture of quantum correlations in pure three-mode Gaussian states, together with the cases of tripartite Bell nonlocality in terms of maximum violation of the Svetlichny inequality [12] and genuine tripartite entanglement in terms of Gaussian Rényi-2 entanglement [12]. Bisymmetric states maximize all three forms of nonclassical correlations; compare, e.g., our Fig. 1(a) with Figs. 1(a) and 1(b) in [12].

Figure 1(b) presents the RGS measure for Gaussian states generated by three squeezed vacuum fields (one in momentum, two in position) with experimentally feasible squeezing parameter $r = 0.345$ (i.e., 3 dB of squeezing) [20,73,74] injected at two beamsplitters with reflectivities R and R' as depicted in the inset of Fig. 1(b), setting $R' = 1/2$ so that $a = \sqrt{1+2R(1-R)(\cosh 4r - 1)}$, $b = c = \sqrt{[1+R^2-(R^2-1)\cosh 4r]/2}$. When $R = 1/3$, one can generate a permutationally invariant Greenberger-Horne-Zeilinger (GHZ)-like state with $a = b = c$ [3]. As one might expect, the latter states maximize the RGS in this case.

(b) Operational connections to quantum secret sharing. Secret sharing [75,76] is a conventional cryptographic protocol in which a dealer (Alice) wants to share a secret with two players, Bob and Charlie, but with one condition: Bob and Charlie should be unable to individually access the secret (which may involve highly confidential information) and their collaboration would be required in order to prevent wrongdoings.

QSS schemes [64,67,77] have been proposed to securely accomplish this task, by exploiting multipartite entanglement to secure and split the classical secret among the players in a single go. Very recently, we provided an unconditional security proof for entanglement-based QSS protocols in a companion paper [66]. In our scheme, the goal of the dealer is to establish a secret key with a joint degree of freedom of the players. The players can only retrieve Alice's key and decode the classical secret by collaborating and communicating to each other their local measurements to form the joint variable. The unconditional security of these schemes stems from the utilized partially device-independent setting, treating the dealer as a trusted party with characterized devices, and the (potentially, dishonest) players as untrusted parties whose measuring devices are described as black boxes. Given this intrinsically asymmetric separation of roles, one would expect that multipartite steering be closely related to the security figure of merit of QSS. Here we prove such a connection quantitatively.

To start with, let us assume that the dealer, Alice, and the players, Bob and Charlie, all perform homodyne measurements of the quadratures $\hat{x}_i, \hat{p}_i$ with outcomes X_i, P_i, with $i = A,B,C$, on the shared tripartite state. Following [66], a guaranteed (asymptotic) secret key rate for the QSS protocol (extracted from the correlations of Alice's momentum detection P_A and a joint variable $\bar{P}$ for Bob and Charlie) to provide security against external eavesdropping is given by $K_E^{A\to\{B,C\}} \geqslant -\ln(e\sqrt{V_{P_A|\bar{P}} V_{X_A|\bar{X}}})$, while the key rate providing *unconditional* security against both eavesdropping and dishonest actions of the players is

$$K_{\text{full}}^{A\to\{B,C\}} \geqslant -\ln\left(e\sqrt{V_{P_A|\bar{P}}\max\{V_{X_A|X_C}, V_{X_A|X_B}\}}\right). \quad (7)$$

Here, $V_{P_A|\bar{P}} = \int d\bar{P}\, p(\bar{P})(\langle P_A^2\rangle_{\bar{P}} - \langle P_A\rangle_{\bar{P}}^2)$ is the minimum inference variance of Alice's momentum outcome given the players' joint outcome $\bar{P}$, and similarly for the other variances. A tripartite shared state ρ_{ABC} whose correlations result in nonzero values of the right-hand side of (7) can be regarded a useful resource for unconditionally secure QSS.

We focus on pure three-mode Gaussian states with CM $\sigma^{\text{pure}}_{ABC}$ in standard form, fully specified by the local invariants a,b,c as before. Our first observation is that K_E is directly quantified by the collective steering, $\mathcal{G}^{(BC)\to A}(\sigma^{\text{pure}}_{ABC}) =$

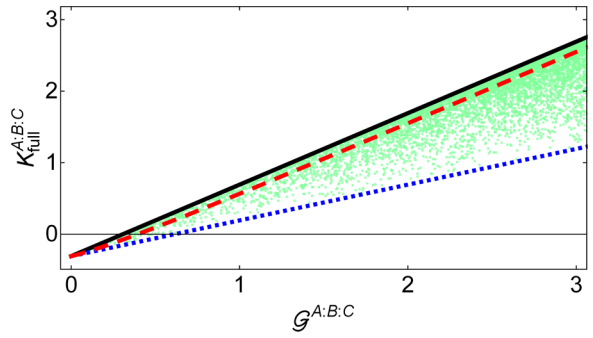

FIG. 2. Mode-invariant secure QSS key rate versus RGS for 10^5 pure three-mode Gaussian states (dots); see text for details on the lines.

$\max\{0, \frac{1}{2}\ln\frac{\det\sigma_{BC}}{\det\sigma_{ABC}}\}$. For the considered class of states, one has indeed $\frac{\det\sigma_{ABC}}{\det\sigma_{BC}} = 4V_{P_A|\bar{P}}V_{X_A|\bar{X}} = 1/a^2$, where the joint variables were chosen to have the linear form $\bar{X} = g_X X_B + h_X X_C$ and $\bar{P} = g_P P_B + h_P P_C$, with the real constants $g_{X(P)}, h_{X(P)}$ optimized as to minimize the inferred variances $V_{X_A|\bar{X}}, V_{P_A|\bar{P}}$ (see also [36,40]). Putting everything together, we get $K_E^{A\to\{B,C\}}(\sigma^{\text{pure}}_{ABC}) \geqslant \max\{0, \mathcal{G}^{(BC)\to A}(\sigma^{\text{pure}}_{ABC}) - \ln\frac{e}{2}\}$.

We can now define a mode-invariant QSS key rate bound $K^{A:B:C}_{\text{full}}$ that takes into account eavesdropping and potential dishonesty of the players, by minimizing the right-hand side of Eq. (7) over the choice of the dealer, i.e., over permutations of A, B, and C. A nonzero value of the figure of merit $K^{A:B:C}_{\text{full}}(\sigma_{ABC})$ on a tripartite Gaussian state with CM σ_{ABC} guarantees the usefulness of the state for unconditionally secure QSS, for any possible assignment of the roles. For pure three-mode Gaussian states, the mode-invariant key rate $K^{A:B:C}_{\text{full}}(\sigma^{\text{pure}}_{ABC})$ can be evaluated explicitly (although its lengthy expression is omitted here) and analyzed in the physical space of the parameters a,b,c. We find that $K^{A:B:C}_{\text{full}}(\sigma^{\text{pure}}_{ABC})$ admits *exact linear upper and lower bounds* as a function of the RGS $\mathcal{G}^{A:B:C}(\sigma^{\text{pure}}_{ABC})$, for all states with standard form CM $\sigma^{\text{pure}}_{ABC}$:

$$\frac{\mathcal{G}^{A:B:C}(\sigma^{\text{pure}}_{ABC})}{2} - \ln\frac{e}{2} \leqslant K^{A:B:C}_{\text{full}}(\sigma^{\text{pure}}_{ABC}) \leqslant \mathcal{G}^{A:B:C}(\sigma^{\text{pure}}_{ABC}) - \ln\frac{e}{2}. \quad (8)$$

The bounds are illustrated in Fig. 2 together with a numerical exploration of 10^5 randomly generated pure three-mode Gaussian states. Remarkably, the bounds are tight, and families of states saturating them can be readily provided. Specifically, the lower (dotted blue) boundary is spanned by states with $a \geqslant 1$, $b = c = (a+1)/2$; conversely, the upper (solid black) boundary is spanned by states with $a \geqslant 1$, $b = c \to \infty$. While these cases are clearly extremal, GHZ-like states (dashed red), specified by $a = b = c$ and producible as discussed in Fig. 1(b), nearly maximize the QSS key rate at fixed RGS, thus arising as convenient practical resources for the considered task, independently of the distribution of trust. Indeed, a squeezing level of 4.315 dB, referring to the scheme of Fig. 1(b), is required to ensure a nonzero key rate using these states. This is well within the current experimental feasibility, since up to 10 dB of squeezing has been demonstrated [73,74]. In general, by imposing non-negativity of the lower bound in (8), we find that $K^{A:B:C}_{\text{full}}(\sigma^{\text{pure}}_{ABC}) > 0$ for all pure three-mode Gaussian states with RGS $\mathcal{G}^{A:B:C}(\sigma^{\text{pure}}_{ABC}) > 2\ln(e/2) \approx 0.614$. Our analysis reveals that partially device-independent QSS is empowered by multipartite steering, yielding a direct operational interpretation for the RGS in terms of the guaranteed key rate of the protocol.

(c) Discussion and conclusion. We have proven that a recently proposed measure of quantum steering under Gaussian measurements [36,42] obeys CKW-type monogamy inequalities for all Gaussian states of any number of modes. We remark that monogamy extends in fact to arbitrary non-Gaussian states under Gaussian measurements, as it is established solely at the level of covariance matrices. Notice, however, that resorting to non-Gaussian measurements can lead to extra steerability even for Gaussian states [51,78], and might allow circumventing some monogamy constraints [55,71,72].

In the important case of pure three-mode Gaussian states, we demonstrate that the residual steering emerging from the laws of monogamy can act as a quantifier of genuine tripartite steering. The latter measure is endowed with an operational interpretation, as it is shown to provide tight bounds on the mode-invariant key rate of a partially device-independent QSS protocol, whose unconditional security has been very recently investigated [66]. Our study, combined with [66], provides practical recipes demonstrating that an implementation of QSS secure against eavesdropping and potentially dishonest players is feasible with current technology using tripartite Gaussian states and Gaussian measurements [79].

Note added. Recently, monogamy inequalities for multipartite Gaussian steering in the case of more than one mode per party have been investigated in [80].

Acknowledgments. Y.X. and Q.H. acknowledge the support of the National Natural Science Foundation of China under Grants No. 11622428, No. 61475006, and No. 61675007. I.K. and G.A. acknowledge funding from the European Research Council under Starting Grant No. 637352 (GQCOP). G.A. thanks R. Simon and L. Lami for useful discussions.

Appendix A: Proof of (2). It suffices to prove the inequality for tripartite states as in (4), with C being a single mode and A,B comprising an arbitrary number of modes. One can then apply iteratively this inequality to obtain the corresponding m-partite one (2).

To do so, recall that from [55,71,72] it is impossible for A and B to simultaneously steer the one-mode party C, that is, $\mathcal{G}^{A\to C}(\sigma_{ABC}) > 0$ implies $\mathcal{G}^{B\to C}(\sigma_{ABC}) = 0$ (and vice versa). Therefore, the monogamy relation (4) reduces to $\mathcal{G}^{(AB)\to C}(\sigma_{ABC}) - \mathcal{G}^{A\to C}(\sigma_{ABC}) \geqslant 0$ (or the analogous expression with swapped $A \leftrightarrow B$), which holds true because the Gaussian steering measure (for one-mode steered party C) is nonincreasing under local Gaussian operations on the steering party (AB) [42], which include discarding B (or A). This proves Eq. (2) for any m-mode CM $\sigma_{A_1\ldots A_m}$. ■

Appendix B: Proof of (3). In this case we have to recall the explicit expression of the Gaussian steering measure [42], defined for a bipartite $(n_A + n_B)$-mode state with CM σ_{AB} as

$$\mathcal{G}^{A\to B}(\sigma_{AB}) = \begin{cases} 0, & \bar{\nu}_j^{AB\setminus A} \geqslant 1 \,\forall j = 1,\ldots,n_B; \\ -\sum_{j:\bar{\nu}_j^{AB\setminus A}<1} \ln\left(\bar{\nu}_j^{AB\setminus A}\right), & \text{otherwise,} \end{cases}$$

where $\{\bar{\nu}_j^{AB\backslash A}\}_{j=1}^{n_B}$ denote the symplectic eigenvalues of the Schur complement $\bar{\sigma}_{AB\backslash A}$ of σ_A in σ_{AB}. By definition of the Schur complement, and observing that $\bar{\sigma}_{AB\backslash A} > 0$ for any valid CM σ_{AB}, notice that we can write $\sqrt{(\det\sigma_{AB})/(\det\sigma_A)} = \sqrt{\det\bar{\sigma}_{AB\backslash A}} = \prod_{j=1}^{n_B}\bar{\nu}_j^{AB\backslash A} = (\prod_{j:\bar{\nu}_j^{AB\backslash A}<1}\bar{\nu}_j^{AB\backslash A})(\prod_{j:\bar{\nu}_j^{AB\backslash A}\geqslant 1}\bar{\nu}_j^{AB\backslash A}) \geqslant (\prod_{j:\bar{\nu}_j^{AB\backslash A}<1}\bar{\nu}_j^{AB\backslash A})$.

Applying $(-\ln)$ to both sides we get, for any CM σ_{AB} with $\mathcal{G}^{A\to B}(\sigma_{AB}) > 0$, the bound (tight when $n_B = 1$ [42])

$$2\mathcal{G}^{A\to B}(\sigma_{AB}) \geqslant \mathcal{M}(\sigma_A) - \mathcal{M}(\sigma_{AB}) = -\mathcal{I}_{B|A}(\sigma_{AB}), \quad \text{(B1)}$$

where $\mathcal{M}(\sigma) = \ln\det\sigma$ is the log-determinant of the CM σ [72], and $\mathcal{I}_{B|A}(\sigma_{AB}) = \mathcal{M}(\sigma_{AB}) - \mathcal{M}(\sigma_A)$ is the conditional log-determinant, which—in analogy to the standard conditional quantum entropy—is concave on the set of CMs [72] and subadditive with respect to the conditioned subsystems,

$$\mathcal{I}_{BC|A}(\sigma_{ABC}) \leqslant \mathcal{I}_{B|A}(\sigma_{ABC}) + \mathcal{I}_{C|A}(\sigma_{ABC}). \quad \text{(B2)}$$

Notice that the latter property is equivalent to the strong subadditivity for the log-determinant of the CM σ_{ABC} [62,72].

To prove (3), it suffices to consider the case in which the multimode term $\mathcal{G}^{A_k\to(A_1,\ldots,A_{k-1},A_{k+1},\ldots,A_m)}$ and all the pairwise terms $\mathcal{G}^{A_k\to A_j}$ are nonzero. Applying then (B1) to the first term in (3), and using repeatedly the negation of (B2), we get $\mathcal{G}^{A_k\to(A_1,\ldots,A_{k-1},A_{k+1},\ldots,A_m)}(\sigma_{A_1\ldots A_m}) \geqslant \frac{1}{2}[\mathcal{M}(\sigma_{A_1,\ldots,A_{k-1},A_{k+1},\ldots,A_m}) - \mathcal{M}(\sigma_{A_1\ldots A_m})] = -\frac{1}{2}\mathcal{I}_{(A_1,\ldots,A_{k-1},A_{k+1},\ldots,A_m)|A_k}(\sigma_{A_1,\ldots,A_m}) \geqslant -\frac{1}{2}\sum_{j\neq k}\mathcal{I}_{A_j|A_k}(\sigma_{A_1\ldots A_m}) = \sum_{j\neq k}\mathcal{G}^{A_k\to A_j}(\sigma_{A_1\ldots A_m})$, where in the last step we used again (B1) which holds with equality on each of the two-mode terms involving A_k and any A_j, provided $\mathcal{G}^{A_k\to A_j}(\sigma_{A_1\ldots A_m}) > 0$ as per assumption. This concludes the proof of Eq. (3) for any m-mode CM $\sigma_{A_1\ldots A_m}$. ■

[1] H. J. Kimble, Nature (London) **453**, 1023 (2008).
[2] P. van Loock and A. Furusawa, Phys. Rev. A **67**, 052315 (2003).
[3] P. van Loock and S. L. Braunstein, Phys. Rev. Lett. **84**, 3482 (2000).
[4] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Rev. Mod. Phys. **81**, 865 (2009).
[5] O. Gühne and G. Tóth, Phys. Rep. **474**, 1 (2009).
[6] G. Adesso and F. Illuminati, New J. Phys. **8**, 15 (2006).
[7] G. Adesso, A. Serafini, and F. Illuminati, Phys. Rev. A **73**, 032345 (2006).
[8] J.-D. Bancal, N. Gisin, Y.-C. Liang, and S. Pironio, Phys. Rev. Lett. **106**, 250404 (2011).
[9] G. Svetlichny, Phys. Rev. D **35**, 3066 (1987).
[10] D. Collins, N. Gisin, S. Popescu, D. Roberts, and V. Scarani, Phys. Rev. Lett. **88**, 170405 (2002).
[11] M. Seevinck and G. Svetlichny, Phys. Rev. Lett. **89**, 060401 (2002).
[12] G. Adesso and S. Piano, Phys. Rev. Lett. **112**, 010401 (2014).
[13] L. K. Shalm, D. R. Hamel, Z. Yan, C. Simon, K. J. Resch, and T. Jennewein, Nat. Phys. **9**, 19 (2013).
[14] Y.-F. Huang, B.-H. Liu, L. Peng, Y.-H. Li, L. Li, C.-F. Li, and G.-C. Guo, Nat. Commun. **2**, 546 (2011).
[15] X.-C. Yao, T.-X. Wang, P. Xu, H. Lu, G.-S. Pan, X.-H. Bao, C.-Z. Peng, C.-Y. Lu, Y.-A. Chen, and J.-W. Pan, Nat. Photonics **6**, 225 (2012).
[16] J. Lavoie, R. Kaltenbaek, and K. J. Resch, New J. Phys. **11**, 073051 (2009).
[17] C. Erven, E. Meyer-Scott, K. Fisher, J. Lavoie, B. Higgins, Z. Yan, C. Pugh, J.-P. Bourgoin, R. Prevedel, L. Shalm *et al.*, Nat. Photonics **8**, 292 (2014).
[18] T. Monz, P. Schindler, J. T. Barreiro, M. Chwalla, D. Nigg, W. A. Coish, M. Harlander, W. Hänsel, M. Hennrich, and R. Blatt, Phys. Rev. Lett. **106**, 130506 (2011).
[19] S. Armstrong, J.-F. Morizur, J. Janousek, B. Hage, N. Treps, P. K. Lam, and H.-A. Bachor, Nat. Commun. **3**, 1026 (2012).
[20] J. Jing, J. Zhang, Y. Yan, F. Zhao, C. Xie, and K. Peng, Phys. Rev. Lett. **90**, 167903 (2003).
[21] X. Su, A. Tan, X. Jia, J. Zhang, C. Xie, and K. Peng, Phys. Rev. Lett. **98**, 070502 (2007).
[22] S. Yokoyama, R. Ukai, S. Armstrong, C. Sornphiphatphong, T. Kaji, S. Suzuki, J.-i. Yoshikawa, H. Yonezawa, N. C. Menicucci, and A. Furusawa, Nat. Photonics **7**, 982 (2013).
[23] C.-M. Li, K. Chen, Y.-N. Chen, Q. Zhang, Y.-A. Chen, and J.-W. Pan, Phys. Rev. Lett. **115**, 010402 (2015).
[24] S. Armstrong, M. Wang, R. Y. Teh, Q. H. Gong, Q. Y. He, J. Janousek, H.-A. Bachor, M. D. Reid, and P. K. Lam, Nat. Phys. **11**, 167 (2015).
[25] E. Schrödinger, Math. Proc. Cambridge Philos. Soc. **31**, 555 (1935).
[26] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).
[27] M. D. Reid, Phys. Rev. A **40**, 913 (1989).
[28] M. D. Reid, P. D. Drummond, W. P. Bowen, E. G. Cavalcanti, P. K. Lam, H. A. Bachor, U. L. Andersen, and G. Leuchs, Rev. Mod. Phys. **81**, 1727 (2009).
[29] H. M. Wiseman, S. J. Jones, and A. C. Doherty, Phys. Rev. Lett. **98**, 140402 (2007).
[30] S. J. Jones, H. M. Wiseman, and A. C. Doherty, Phys. Rev. A **76**, 052116 (2007).
[31] S. P. Walborn, A. Salles, R. M. Gomes, F. Toscano, and P. H. Souto Ribeiro, Phys. Rev. Lett. **106**, 130402 (2011).
[32] V. Händchen, T. Eberle, S. Steinlechner, A. Samblowski, T. Franz, R. F. Werner, and R. Schnabel, Nat. Photonics **6**, 596 (2012).
[33] J. Bowles, T. Vértesi, M. T. Quintino, and N. Brunner, Phys. Rev. Lett. **112**, 200402 (2014).
[34] M. T. Quintino, T. Vértesi, D. Cavalcanti, R. Augusiak, M. Demianowicz, A. Acín, and N. Brunner, Phys. Rev. A **92**, 032107 (2015).
[35] Q. Y. He, Q. H. Gong, and M. D. Reid, Phys. Rev. Lett. **114**, 060402 (2015).
[36] I. Kogias, A. R. Lee, S. Ragy, and G. Adesso, Phys. Rev. Lett. **114**, 060403 (2015).
[37] I. Kogias, P. Skrzypczyk, D. Cavalcanti, A. Acín, and G. Adesso, Phys. Rev. Lett. **115**, 210401 (2015).

[38] E. G. Cavalcanti, S. J. Jones, H. M. Wiseman, and M. D. Reid, Phys. Rev. A **80**, 032112 (2009).
[39] C. Branciard, E. G. Cavalcanti, S. P. Walborn, V. Scarani, and H. M. Wiseman, Phys. Rev. A **85**, 010301 (2012).
[40] N. Walk, S. Hosseini, J. Geng, O. Thearle, J. Y. Haw, S. Armstrong, S. M. Assad, J. Janousek, T. C. Ralph, T. Symul, H. M. Wiseman, and P. K. Lam, Optica **3**, 634 (2016).
[41] P. Skrzypczyk, M. Navascués, and D. Cavalcanti, Phys. Rev. Lett. **112**, 180404 (2014).
[42] I. Kogias and G. Adesso, J. Opt. Soc. Am. B **32**, A27 (2015).
[43] A. C. S. Costa and R. M. Angelo, Phys. Rev. A **93**, 020103 (2016).
[44] Q. Y. He, L. Rosales-Zárate, G. Adesso, and M. D. Reid, Phys. Rev. Lett. **115**, 180502 (2015).
[45] D. J. Saunders, S. J. Jones, H. M. Wiseman, and G. J. Pryde, Nat. Phys. **6**, 845 (2010).
[46] A. J. Bennet, D. A. Evans, D. J. Saunders, C. Branciard, E. G. Cavalcanti, H. M. Wiseman, and G. J. Pryde, Phys. Rev. X **2**, 031003 (2012).
[47] B. Wittmann, S. Ramelow, F. Steinlechner, N. K. Langford, N. Brunner, H. M. Wiseman, R. Ursin, and A. Zeilinger, New J. Phys. **14**, 053030 (2012).
[48] K. Sun, X.-J. Ye, J.-S. Xu, X.-Y. Xu, J.-S. Tang, Y.-C. Wu, J.-L. Chen, C.-F. Li, and G.-C. Guo, Phys. Rev. Lett. **116**, 160404 (2016).
[49] K. Sun, J.-S. Xu, X.-J. Ye, Y.-C. Wu, J.-L. Chen, C.-F. Li, and G.-C. Guo, Phys. Rev. Lett. **113**, 140402 (2014).
[50] S. Kocsis, M. J. Hall, A. J. Bennet, D. J. Saunders, and G. J. Pryde, Nat. Commun. **6**, 5886 (2015).
[51] S. Wollmann, N. Walk, A. J. Bennet, H. M. Wiseman, and G. J. Pryde, Phys. Rev. Lett. **116**, 160403 (2016).
[52] Q. Y. He and M. D. Reid, Phys. Rev. Lett. **111**, 250403 (2013).
[53] R. Y. Teh and M. D. Reid, Phys. Rev. A **90**, 062337 (2014).
[54] D. Cavalcanti, P. Skrzypczyk, G. Aguilar, R. Nery, P. S. Ribeiro, and S. Walborn, Nat. Commun. **6**, 7941 (2015).
[55] M. D. Reid, Phys. Rev. A **88**, 062108 (2013).
[56] G. Adesso and F. Illuminati, J. Phys. A: Math. Theor. **40**, 7821 (2007).
[57] 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).
[58] *Quantum Information with Continuous Variables of Atoms and Light*, edited by N. Cerf, G. Leuchs, and E. S. Polzik (Imperial College Press, London, 2007).
[59] V. Coffman, J. Kundu, and W. K. Wootters, Phys. Rev. A **61**, 052306 (2000).
[60] T. Hiroshima, G. Adesso, and F. Illuminati, Phys. Rev. Lett. **98**, 050503 (2007).
[61] T. J. Osborne and F. Verstraete, Phys. Rev. Lett. **96**, 220503 (2006).
[62] G. Adesso, D. Girolami, and A. Serafini, Phys. Rev. Lett. **109**, 190502 (2012).
[63] C. Lancien, S. Di Martino, M. Huber, M. Piani, G. Adesso, and A. Winter, Phys. Rev. Lett. **117**, 060501 (2016).
[64] M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).
[65] H.-K. Lau and C. Weedbrook, Phys. Rev. A **88**, 042313 (2013).
[66] I. Kogias, Y. Xiang, Q. Y. He, and G. Adesso, Phys. Rev. A **95**, 012315 (2017).
[67] Here QSS is intended as quantum sharing of a classical secret, not to be confused with sharing a quantum state as in [68].
[68] R. Cleve, D. Gottesman, and H.-K. Lo, Phys. Rev. Lett. **83**, 648 (1999).
[69] B. M. Terhal, IBM J. Res. Dev. **48**, 71 (2004).
[70] G. Adesso and F. Illuminati, Phys. Rev. Lett. **99**, 150501 (2007).
[71] S.-W. Ji, M. S. Kim, and H. Nha, J. Phys. A: Math. Theor. **48**, 135301 (2015).
[72] G. Adesso and R. Simon, J. Phys. A: Math. Theor. **49**, 34LT02 (2016).
[73] Y. Zhou, X. Jia, F. Li, C. Xie, and K. Peng, Opt. Express **23**, 4952 (2015).
[74] T. Eberle, V. Händchen, and R. Schnabel, Opt. Express **21**, 11546 (2013).
[75] A. Shamir, Commun. ACM **22**, 612 (1979).
[76] G. R. Blakley, in *afips* (IEEE, New York, 1899), p. 313.
[77] A. Karlsson, M. Koashi, and N. Imoto, Phys. Rev. A **59**, 162 (1999).
[78] S.-W. Ji, J. Lee, J. Park, and H. Nha, Sci. Rep. **6**, 29729 (2016).
[79] In the recent experiment of Ref. [24] the principles of partially device-independent QSS were presented, but our present analysis allows us to conclude that the achieved level of steering was not sufficient to obtain a key rate above the unconditional security threshold in that case.
[80] L. Lami, C. Hirche, G. Adesso, and A. Winter, Phys. Rev. Lett. **117**, 220502 (2016).