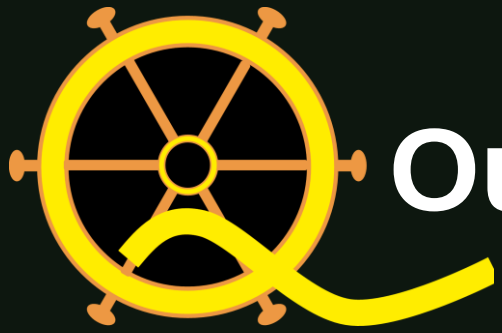
The University of Nottingham
UNITED KINGDOM · CHINA · MALAYSIA

Multipartite steering of Gaussian states

monogamy constraints and cryptographical applications

Gerardo Adesso

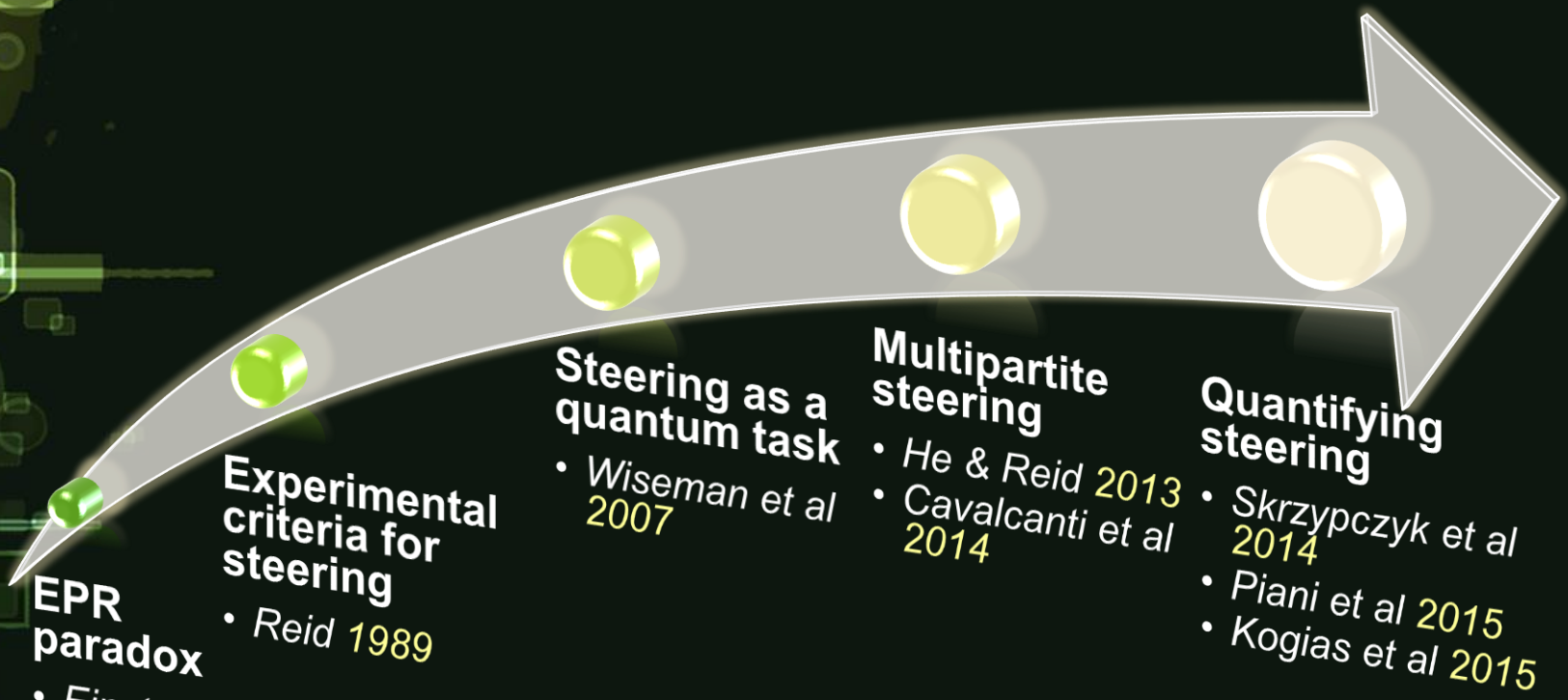
Quantum Correlations Group
The University of Nottingham



Outline

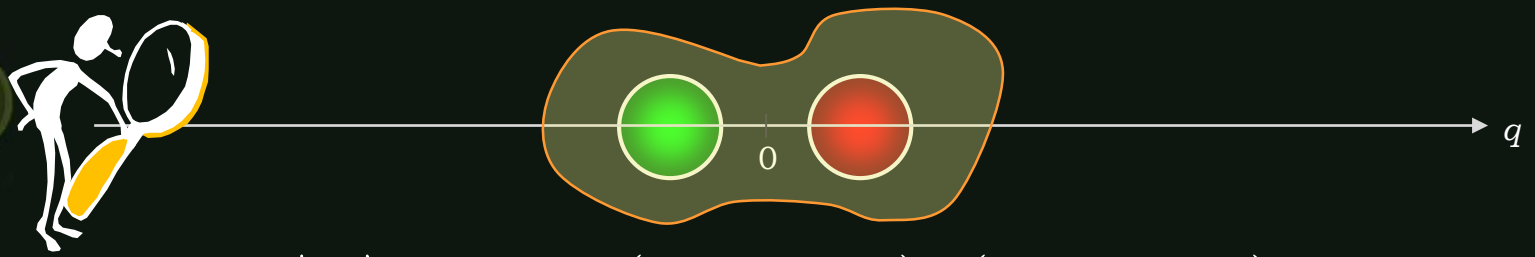
- Einstein-Podolsky-Rosen steering
- Bipartite Gaussian steering
- Multipartite Gaussian steering
- Monogamy and residual steering
- Security of quantum secret sharing
- Conclusions

Steering timeline



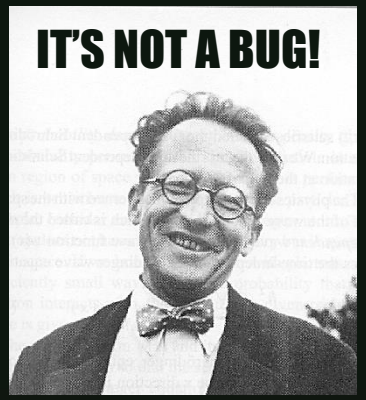
Review: *Cavalcanti & Skrzypczyk arXiv:1604.0050 2016*

EPR paradox (1935)



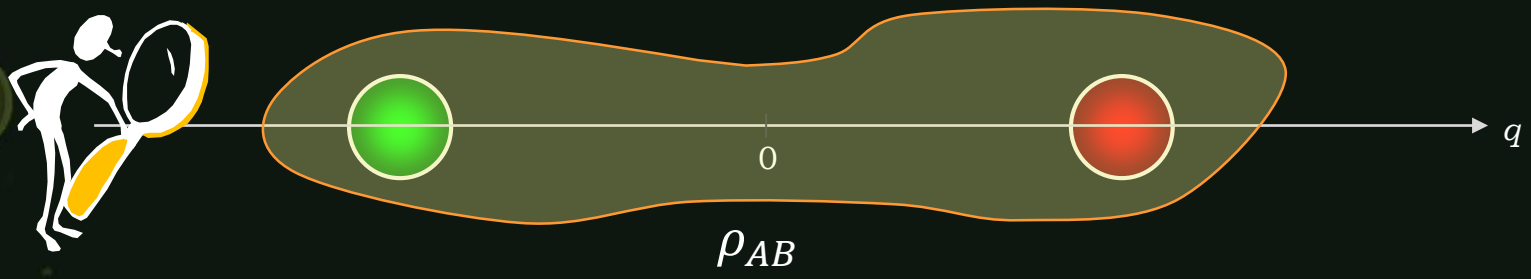
$$|\psi\rangle_{AB} \sim \delta(\hat{q}_A - \hat{q}_B)\delta(\hat{p}_A + \hat{p}_B)$$

"As a consequence of two different measurements performed upon the first system, the second system may be left in states with two different [kinds of] wavefunctions"



*"The theory allows a system to be **steered** into one or the other type of state at the experimenter's mercy in spite of his having no access to it. […] Since I can predict either [q] or [p] without interfering with [the second] system, [it] must know both answers; which is an amazing knowledge."*

Reid's criterion (1989)



- Bob can measure $\hat{q}_B$ or $\hat{p}_B$, obtaining respective outcomes Q_B, P_B
- Alice wants to guess those outcomes by measuring her system
- Alice measures $\hat{q}_A$ with outcome Q_A and infers $Q_B^{est}(Q_A)$ e.g. by linear inference, $Q_B^{est}(Q_A) = g_q Q_A + d_q$
- The inferred variance on Bob's outcome given Alice's estimate is $\Delta^2_{Q_B|Q_A} = \langle [Q_B - Q_B^{est}(Q_A)]^2 \rangle$ and it can be minimised by finding the optimal g_q, d_q
- Alice can equivalently estimate P_B by measuring $\hat{p}_A$

Criterion: If the Heisenberg-type condition

$$\Delta^2_{Q_B|Q_A}\ \Delta^2_{P_B|P_A} \geq 1$$

is violated, then ρ_{AB} is *"$A \to B$ steerable"*

Wiseman *et al.* (2007)

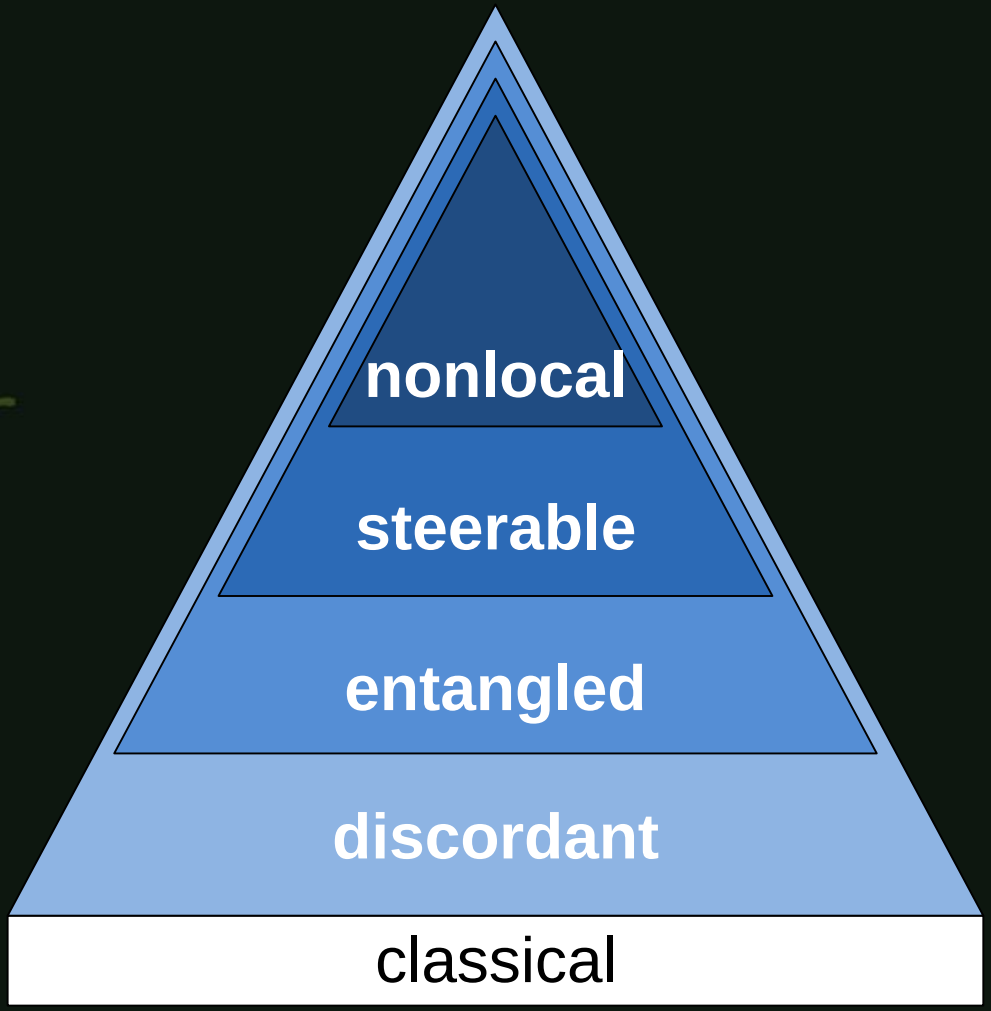
For a bipartite state ρ_{AB}, given measurement operators $\hat{a}$ and $\hat{b}$ on Alice's and Bob's parties, with outcomes A and B, if for all pairs $\hat{a}$ and $\hat{b}$ the joint statistics of the measurement results cannot

- have arisen from correlations between a random local hidden variable for Alice and a random local hidden variable for Bob,
$$p(A,B|\hat{a},\hat{b};\rho_{AB}) \neq \sum_\lambda p(A|\hat{a},\lambda)\, p(B|\hat{b},\lambda)\, p_\lambda$$
$\Rightarrow \rho_{AB}$ is ***Bell nonlocal***

- have arisen from correlations between a random local hidden variable for Alice and a local hidden state measured by Bob,
$$p(A,B|\hat{a},\hat{b};\rho_{AB}) \neq \sum_\lambda p(A|\hat{a},\lambda) p(B|\hat{b};\tau_\lambda^B)\, p_\lambda$$
$\Rightarrow \rho_{AB}$ is ***A → B steerable***

- have arisen from correlations between a random pure state measured by Alice and a random pure state measured by Bob,
$$p(A,B|\hat{a},\hat{b};\rho_{AB}) \neq \sum_\lambda p(\hat{a}|A;\sigma_\lambda^A) p(B|\hat{b};\tau_\lambda^B)\, p_\lambda$$
$\Rightarrow \rho_{AB}$ is ***entangled***

Hierarchy of correlations



Continuous variable systems

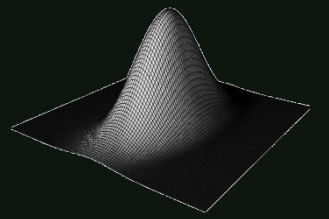
$$\hat{H} = \sum_{k=1}^{N} \hbar\omega_k \left(\hat{a}_k^\dagger \hat{a}_k + \frac{1}{2} \right)$$

- We introduce a **vector** of canonical operators:
$$\hat{R} = (\hat{q}_1, \hat{p}_1, \hat{q}_2, \hat{p}_2, \dots, \hat{q}_N, \hat{p}_N),$$
with $\hat{q}_k = \frac{1}{\sqrt{2}}(\hat{a}_k + \hat{a}_k^\dagger),\ \hat{p}_k = \frac{1}{i\sqrt{2}}(\hat{a}_k - \hat{a}_k^\dagger)$

- Canonical commutation relations: $[\hat{q}_j, \hat{p}_k] = i\,\delta_{jk}$

- Recalling the *N*-mode **symplectic form** $\Omega_N = \Omega^{\oplus N}$, with $\Omega = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, we can write the commutation relations compactly:
$$[\hat{R}_j, \hat{R}_k] = i\,(\Omega_N)_{jk}$$

Gaussian states



- are states whose Wigner distribution is a **Gaussian** function in phase space

$$W_\rho(\xi) = \frac{\exp[-(\xi - \bar{R})^T \boldsymbol{\sigma}^{-1} (\xi - \bar{R})]}{\pi^N \sqrt{\det \boldsymbol{\sigma}}}$$

- Completely specified by:
  - A vector of means $\bar{R}$ (**first moments**): $\bar{R} = \langle \hat{R} \rangle_\rho = (\langle \hat{q}_1 \rangle, \langle \hat{p}_1 \rangle, \ldots, \langle \hat{q}_N \rangle, \langle \hat{p}_N \rangle)$ *[irrelevant: can be set to 0]*
  - A **covariance matrix** (**second moments**) $\boldsymbol{\sigma}$ of elements

$$\sigma_{jk} = \langle \hat{R}_j \hat{R}_k + \hat{R}_k \hat{R}_j \rangle_\rho - 2 \langle \hat{R}_j \rangle_\rho \langle \hat{R}_k \rangle_\rho$$

Gaussian steering

- **Bona fide vs PPT vs steering**

	Physical	PPT	$A \to B$ non-steerable
Density matrix	$\rho_{AB} \geq 0$	$\rho_{AB}^{T_B} \geq 0$	no simple criterion
Covariance matrix	$\sigma_{AB} + i[\Omega_A \oplus \Omega_B] \geq 0$	$\sigma_{AB} + i[(-\Omega_A) \oplus \Omega_B] \geq 0$	$\sigma_{AB} + i[(0_A) \oplus \Omega_B] \geq 0$
Symplectic spectrum	$\nu_k \geq 1 \ \ \forall k$	$\tilde{\nu}_k \geq 1 \ \ \forall k$	???

– Violation of this condition is *necessary and sufficient* for steerability of **all** bipartite Gaussian states by Gaussian measurements *(Wiseman et al PRL 2007)*

Gaussian steering

Recall: $\sigma_{AB} = \begin{pmatrix} \alpha & \gamma \\ \gamma^T & \beta \end{pmatrix}$

Then: $\sigma_{AB} + i[(0_A) \oplus \Omega_B] \geq 0 \Leftrightarrow$

$$\begin{cases} \alpha > 0 \text{ (always true)} \\ \bar{\sigma}_B + i\,\Omega_B \geq 0 \end{cases}$$

where we defined the Schur complement

$\bar{\sigma}_B = \beta - \gamma^T \alpha^{-1} \gamma$

with symplectic spectrum $\{\bar{\nu}_k\}$

Criterion: the bipartite Gaussian state σ_{AB} is $A \to B$ steerable by Gaussian measurements if and only if the Schur covariance matrix $\bar{\sigma}_B$ is not *bona fide*

Gaussian steering: measure

	Physical	PPT	$A \to B$ non-steerable
Covariance matrix	$\sigma_{AB} + i[\Omega_A \oplus \Omega_B] \geq 0$	$\tilde{\sigma}_{AB} + i[\Omega_A \oplus \Omega_B] \geq 0$	$\bar{\sigma}_B + i[\Omega_B] \geq 0$
Symplectic spectrum	$\nu_k \geq 1 \ \ \forall k$ $(k = 1, \dots, n_A + n_B)$	$\tilde{\nu}_k \geq 1 \ \ \forall k$ $(k = 1, \dots, n_A + n_B)$	$\bar{\nu}_k \geq 1 \ \ \forall k$ $(k = 1, \dots, n_B)$

- **Gaussian steerability:**

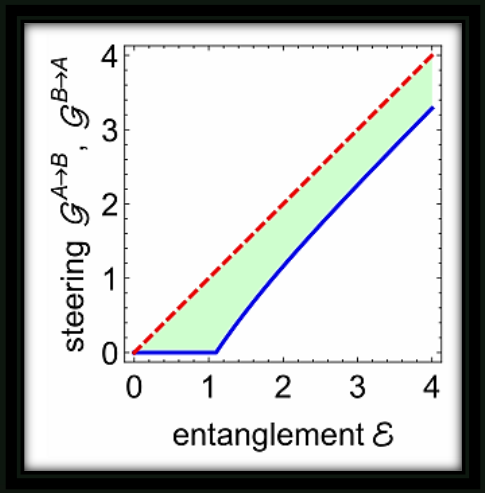
$$\mathcal{G}^{A\to B}(\sigma_{AB}) = \begin{cases} 0, & \text{if } \bar{\nu}_k \geq 1 \ \ \forall k \\ -\sum_{k:\, \bar{\nu}_k < 1} \log \bar{\nu}_k \end{cases}$$

Kogias et al PRL 2015

Gaussian steering: properties

$$\mathcal{G}^{A\to B}(\sigma_{AB}) = \begin{cases} 0, & \text{if } \bar{\nu}_k \geq 1 \ \ \forall k \\ -\sum_{k:\,\bar{\nu}_k<1} \log \bar{\nu}_k \end{cases}$$

- Computable
- Monotone under Gaussian LOCC
- Additive on tensor product states
- Convex
- Equal to Renyi-2 measure of entanglement on pure states
- Smaller than entanglement on mixed states *(i.e. respects the hierarchy of correlations!)*



Gaussian steering: $N \to 1$ modes

- **Gaussian steerability:** $\sigma_{AB} = \begin{pmatrix} \alpha & \gamma \\ \gamma^T & \beta \end{pmatrix}$

$$\mathcal{G}^{A\to B}(\sigma_{AB}) = \max\{0, -\tfrac{1}{2}\log\det\bar{\sigma}_B\}$$
$$= \max\left\{0, \frac{1}{2}\log\frac{\det\alpha}{\det\sigma_{AB}}\right\}$$
$$= \max\{0, S_2(\alpha) - S_2(\sigma_{AB})\}$$

– The degree of steering (by Gaussian measurements) takes the form of a *Renyi-2 coherent information*

Multipartite steering

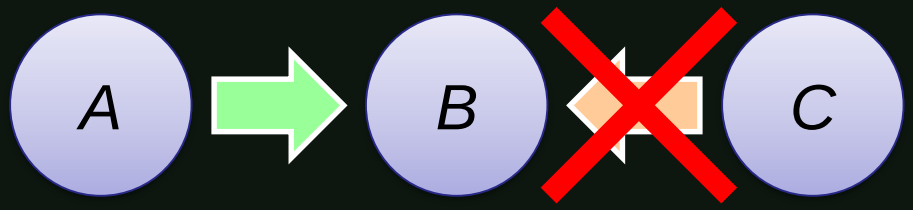
- Different definitions in the literature, depending whether the trusted/untrusted roles of the parties are fixed *(Cavalcanti et al 2015)* or not *(He & Reid 2014).*

- In the latter case, a tripartite state exhibits **genuine tripartite steering** if its correlations rule out a hybrid local-nonlocal hidden state model:

- $p(A,B,C|\hat{a},\hat{b},\hat{c};\rho_{ABC}) \neq P_A \sum_\lambda p(A|\hat{a},\lambda)p(BC|\hat{b},\hat{c};\tau_\lambda^{BC})\ p_\lambda + P_B \sum_\lambda p(B|\hat{b},\lambda)p(CA|\hat{c},\hat{a};\tau_\lambda^{CA})\ p_\lambda + P_C \sum_\lambda p(C|\hat{c},\lambda)p(AB|\hat{a},\hat{b};\tau_\lambda^{AB})\ p_\lambda$ with $P_A + P_B + P_C = 1$

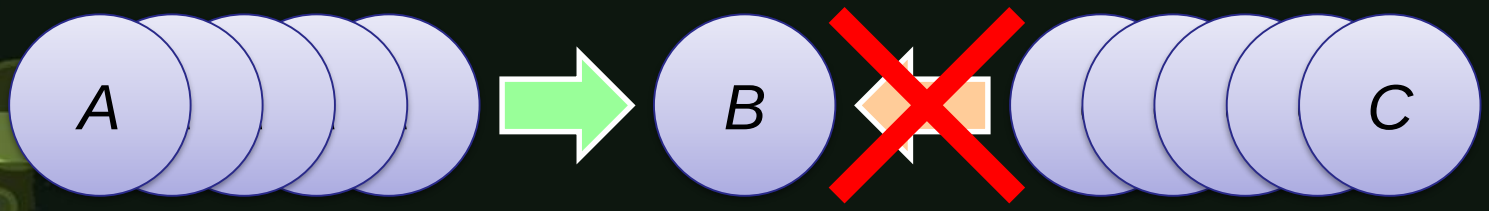
- Sufficient condition: If $A \to BC$ steerable, $B \to AC$ steerable, and $C \to AB$ steerable, then the state possesses genuine tripartite steering

Monogamy



- Reid 2013: $(\Delta^2_{Q_B|Q_A}\ \Delta^2_{P_B|P_A})(\Delta^2_{Q_B|Q_C}\ \Delta^2_{P_B|P_C}) \geq 1$
  - This holds for arbitrary (Gaussian or non-Gaussian) states of three single modes *ABC*
- If *A* steers *B* by Gaussian measurements, then *C* **cannot** steer *B* by Gaussian measurements

Monogamy: extended

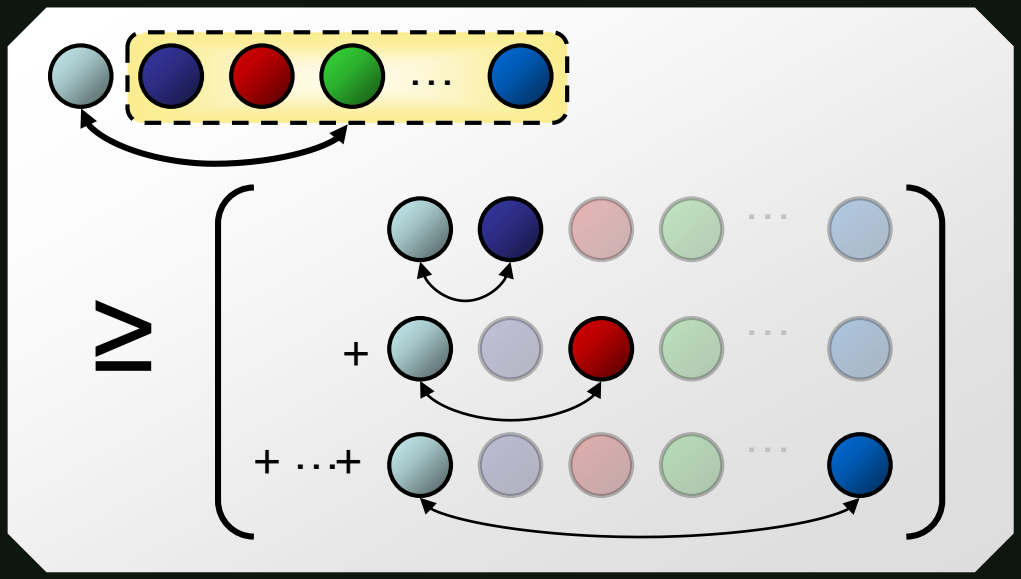


- Two parties *A* and *C* of arbitrarily many modes **cannot** simultaneously steer a third party *B* by using only Gaussian measurements

- The result follows from the **strong subadditivity inequality for log-determinant of covariance matrices** valid for arbitrary tripartite continuous variable states *(GA et al PRL 2012, GA & Simon 2016)*

$$S_2(\sigma_{AB}) + S_2(\sigma_{BC}) - S_2(\sigma_A) - S_2(\sigma_C) \geq 0$$

Monogamy: CKW inequality

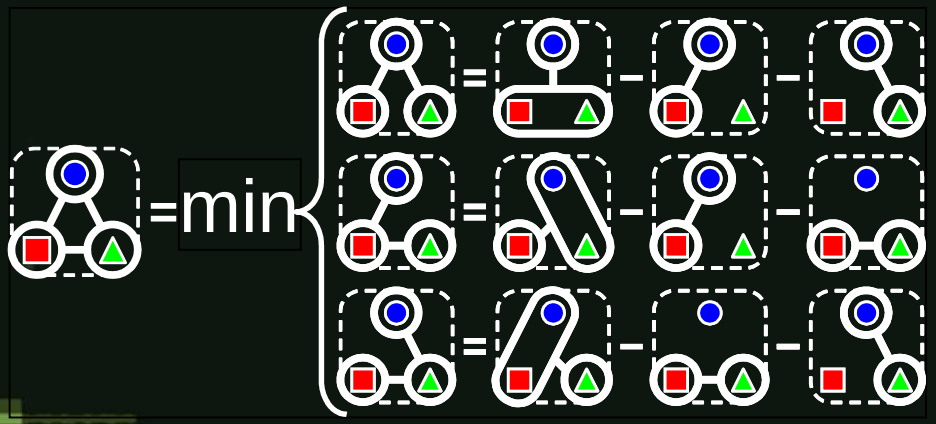


Gaussian steerability is **monogamous** *(Xiang et al 2016)*

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

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

Residual Gaussian steering



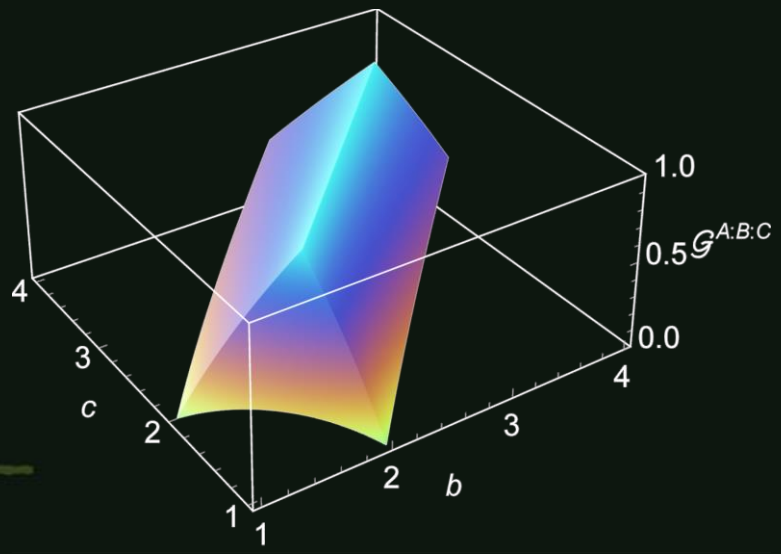
$$\sigma_{ABC} = \begin{pmatrix} \sigma_A & \gamma_{AB} & \gamma_{AC} \\ \gamma_{AB}^T & \sigma_B & \gamma_{BC} \\ \gamma_{AC}^T & \gamma_{BC}^T & \sigma_C \end{pmatrix}$$

For pure 3-mode Gaussian states the residual Gaussian steering (RGS) is independent of the steering direction

$$\mathcal{G}^{A:B:C}\left(\sigma_{ABC}^{\text{pure}}\right) = \min \begin{Bmatrix} \mathcal{G}^{(BC)\to A} - \mathcal{G}^{B\to A} - \mathcal{G}^{C\to A} \\ \mathcal{G}^{(AC)\to B} - \mathcal{G}^{A\to B} - \mathcal{G}^{C\to B} \\ \mathcal{G}^{(AB)\to C} - \mathcal{G}^{A\to C} - \mathcal{G}^{B\to C} \end{Bmatrix}$$

$$= \min \begin{Bmatrix} \mathcal{G}^{A\to (BC)} - \mathcal{G}^{A\to B} - \mathcal{G}^{A\to C} \\ \mathcal{G}^{B\to (AC)} - \mathcal{G}^{B\to A} - \mathcal{G}^{B\to C} \\ \mathcal{G}^{C\to (AB)} - \mathcal{G}^{C\to A} - \mathcal{G}^{C\to B} \end{Bmatrix}$$

Residual Gaussian steering



For pure 3-mode Gaussian states the residual Gaussian steering (RGS) is independent of the steering direction

$$\mathcal{G}^{A:B:C}\left(\sigma_{ABC}^{\text{pure}}\right) = \log \min\left\{\frac{bc}{a}, \frac{ca}{b}, \frac{ab}{c}\right\}$$

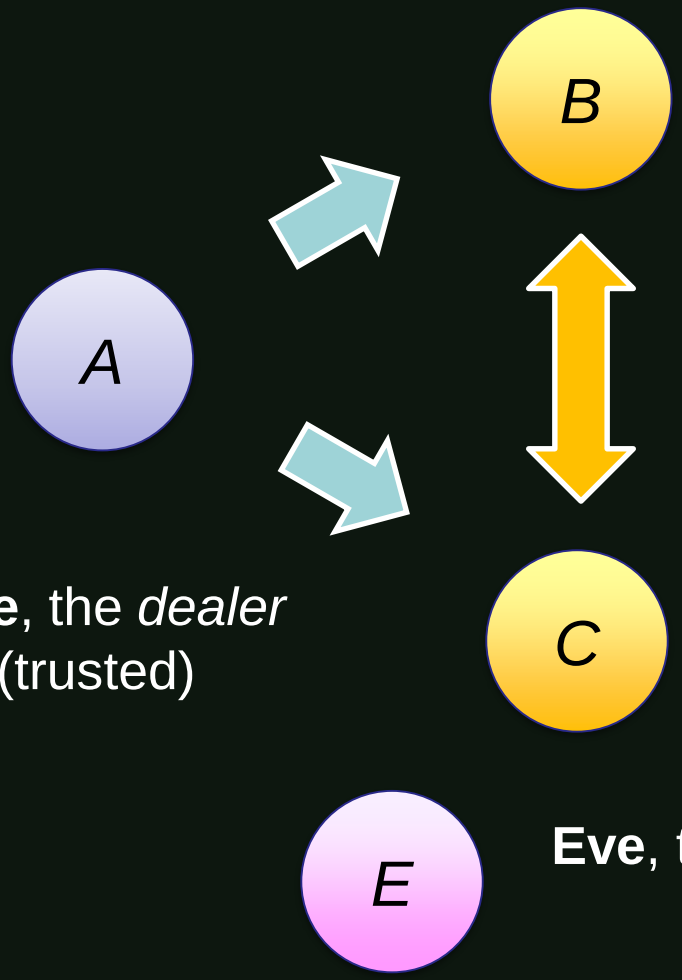
where $a = \sqrt{\det \sigma_A}$, $b = \sqrt{\det \sigma_B}$, $c = \sqrt{\det \sigma_C}$
are constrained to $|b - c| + 1 \leq a \leq b + c - 1$

Applications to cryptography

- **One-sided device independent quantum key distribution (1sDI-QKD)**
  - Alice and Bob share a two-mode Gaussian state (with standard form covariance matrix σ_{AB})
  - Suppose *B* is uncharacterized. Then one can bound the secure key rate in the limit of asymptotically long keys *(Walk et al 2014)*
- **Secure key rate *K* bound**

$$K \geq \max\left\{0, \mathcal{G}^{B\to A}(\sigma_{AB}) - \log\frac{e}{2}\right\}$$

Multipartite: Secret sharing



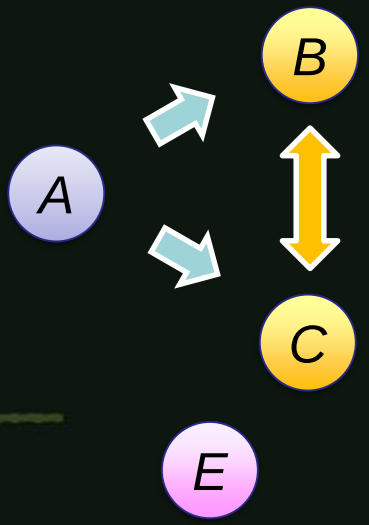
Bob and **Charlie**, the *players* (potentially dishonest, untrusted)

Bob and Charlie cannot access Alice's message individually, but need to cooperate

Alice, the *dealer* (trusted)

Eve, the eavesdropper (untrusted)

Quantum secret sharing



- **Alice, Bob and Charlie share a tripartite entangled state**
- Each can do local **homodyne detections** of $\hat{q}_i, \hat{p}_i$ with outcomes Q_i, P_i on their mode $i = A, B, C$
- The goal is for Alice to establish a secret key with a joint variable $\bar{Q}_{BC}$ or $\bar{P}_{BC}$ for Bob and Charlie

- **Key rate for security against eavesdropping:**

$$K_E^{A\to\{B,C\}} \geq -\log\left(e\, \Delta^2_{P_A|\bar{P}_{BC}}\, \Delta^2_{Q_A|\bar{Q}_{BC}} \right)$$

- **Key rate for unconditional security, including dishonesty of the players** *(Kogias et al 2016)*:

$$K_U^{A\to\{B,C\}} \geq -\log\left(e\, \Delta^2_{P_A|\bar{P}_{BC}}\, \max\left\{ \Delta^2_{Q_A|Q_B}, \Delta^2_{Q_A|Q_C} \right\} \right)$$

Quantum secret sharing

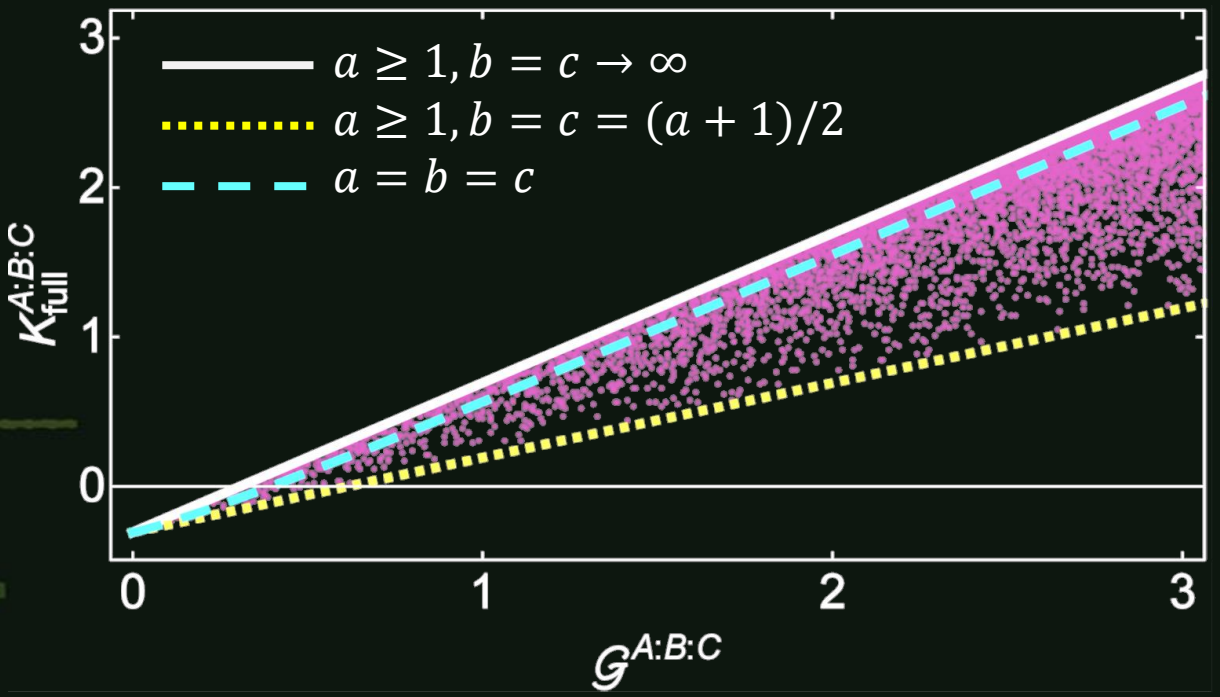
- **Mode-invariant unconditional key rate**

$$K_{\text{full}}^{A:B:C} = \min \left\{ \begin{array}{l} -\log\left(e\, \Delta^2_{P_A|\bar{P}_{BC}} \max\left\{\Delta^2_{Q_A|Q_B}, \Delta^2_{Q_A|Q_C}\right\}\right) \\ -\log\left(e\, \Delta^2_{P_B|\bar{P}_{CA}} \max\left\{\Delta^2_{Q_B|Q_C}, \Delta^2_{Q_B|Q_A}\right\}\right) \\ -\log\left(e\, \Delta^2_{P_C|\bar{P}_{AB}} \max\left\{\Delta^2_{Q_C|Q_A}, \Delta^2_{Q_C|Q_B}\right\}\right) \end{array} \right\}$$

- Any state ρ_{ABC} with $K_{\text{full}}^{A:B:C} > 0$ is a useful **resource** for unconditionally secure quantum secret sharing, *independently of the assignment of the roles*

- The figure of merit $K_{\text{full}}^{A:B:C}$ can be computed **exactly** for pure three-mode Gaussian states with standard form covariance matrix $\sigma_{ABC}^{\text{pure}}$ in terms of a, b, c

Tripartite steering as a resource



- The security figure of merit $K_U^{A:B:C}$ admits tight linear bounds in terms of the **residual Gaussian steering**

$$\frac{1}{2}\mathcal{G}^{A:B:C} - \log\frac{e}{2} \leq K_{\text{full}}^{A:B:C} \leq \mathcal{G}^{A:B:C} - \log\frac{e}{2}$$

Conclusions

- We defined a **Gaussian measure of quantum steering** for bipartite Gaussian states under Gaussian measurements
- We showed that the Gaussian steering obeys generalized **monogamy relations**
- We defined the residual Gaussian steering as a **genuine tripartite steering** indicator
- We operationally linked the residual Gaussian steering to the unconditional security of partially device-independent **quantum secret sharing** schemes

Outlook: Beyond the all-Gaussian world

- Very recently, examples of two-mode Gaussian states have been found, which are unsteerable by Gaussian measurements, yet **steerable by non-Gaussian measurements**

  (Wollman et al arXiv:1511.01231; Ji et al arXiv:1511.02649)

- *Necessary and sufficient condition for steerability of all bipartite Gaussian states (under any measurements)?*

References

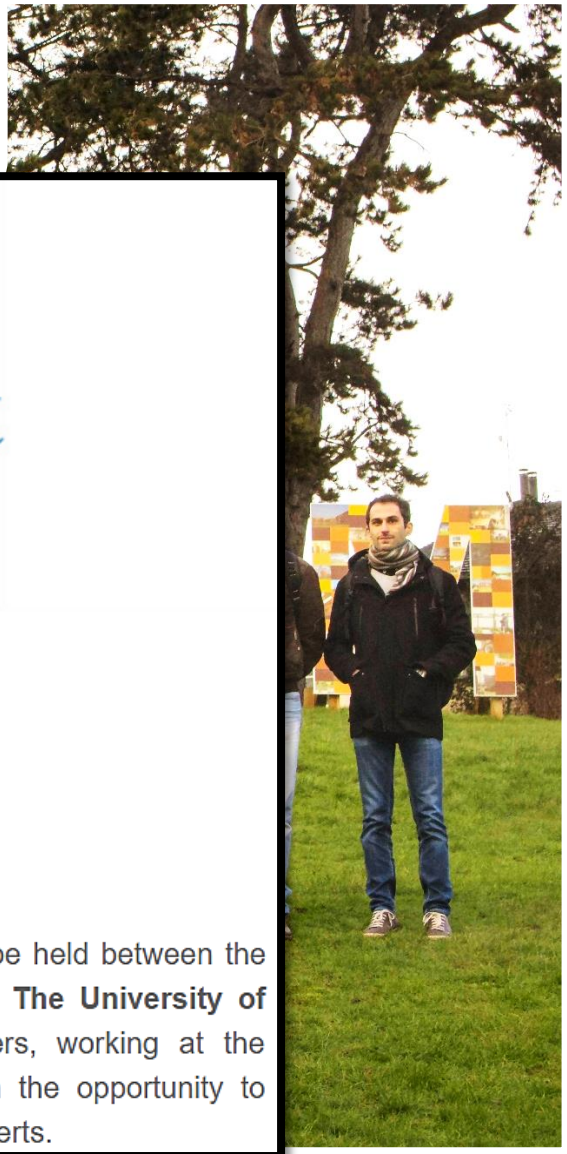
- **Quantification of Gaussian quantum steering**
  - Kogias, Lee, Ragy & Adesso; **Phys. Rev. Lett. 114**, 060403 (2015)
- **EPR-Steering measure for two-mode continuous variable states**
  - Kogias & Adesso; **JOSA B 32**, A27 (2015) *Special Issue*
- **Strong subadditivity for log-determinant of covariance matrices and its applications**
  - Adesso & Simon; **arXiv:1601.03226** (2016)
- **Multipartite Gaussian steering: monogamy constraints and cryptographical applications**
  - Xiang, Kogias, Adesso & He; **arXiv:1603.08173** (2016)
- **Unconditional security of entanglement-based quantum secret sharing schemes**
  - Kogias, Xiang, He & Adesso; **arXiv:1603.03224** (2016)
- **Hierarchy of Steering Criteria Based on Moments for All Bipartite Quantum Systems**
  - Kogias, Skrzypczyk, Cavalcanti, Acin & Adesso **Phys. Rev. Lett. 115**, 210401 (2015)
- **Secure Continuous Variable Teleportation and Einstein-Podolsky-Rosen Steering**
  - He, Rosales-Zarate, Adesso & Reid; **Phys. Rev. Lett. 115**, 180502 (2015)

European Research Council
Established by the European Commission

Thank you

The University of Nottingham

Quantum Correlations Group
The University of Nottingham
http://quantumcorrelations.weebly.com



Quantum Roundabout

Quantum Roundabout

Nottingham, 6th-8th July 2016

http://quantumroundabout.weebly.com

Registration is now open (deadline 29th April)

Quantum Roundabout is a postgraduate conference on quantum physics, to be held between the **6th and 8th of July of 2016** at the **School of Mathematical Sciences** of **The University of Nottingham**. This event intends to bring together early career researchers, working at the crossroads between physics and applied mathematics, providing them with the opportunity to network and interact with their peers in related areas, as well as recognised experts.