Loophole-free EPR-steering and applications

in testing quantum jump subjectivity and in quantum cryptography.

Howard M. Wiseman, and Jay M. Gambetta, and
C. Branciard, E. G. Cavalcanti, S. P. Walborn, and V. Scarani.

Griffith UNIVERSITY

CENTRE FOR QUANTUM COMPUTATION & COMMUNICATION TECHNOLOGY
AUSTRALIAN RESEARCH COUNCIL CENTRE OF EXCELLENCE

Outline

Outline

Three Notions of Nonlocality

1. May 1935, **Einstein, Podolsky & Rosen (EPR correlations):**
   "...as a consequence of two different measurements performed upon the first system, the [distant] second system may be left in states with two different [types of] wavefunctions."

2. November 1935, **Schrödinger's "entanglement of knowledge":**
   "Maximal knowledge of a total system does not necessarily include total knowledge of all its parts, not even when these are fully separated from each other."

3. December 1964, **Bell (Bell nonlocality):**
   "In a theory in which parameters ...determine the results of individual measurements, ...there must be a mechanism whereby the setting of one measurement device can influence the reading of another instrument, however remote."

Why EPR-*Steering*?

EPR introduce a general pure state held by (say) Alice and Bob:

$$|\Psi\rangle = \sum_{n=1}^{\infty} c_n |u_n\rangle|\psi_n\rangle = \sum_{s=1}^{\infty} d_s |v_s\rangle|\varphi_s\rangle. \quad (1)$$

If Alice measures in the $\{|u_n\rangle\}$ (resp. $\{|v_s\rangle\}$) basis, she would instantly collapse Bob's system into one of the states $|\psi_n\rangle$ (resp. $|\varphi_s\rangle$):

> *[A]s a consequence of two different measurements performed upon the first system, the* [distant] *second system may be left in states with two different* [types of] *wavefunctions.*

- Schrödinger (1935) called this **steering** or **piloting** the remote state, and generalized it to arbitrarily many measurements by Alice.

Why EPR-*Steering*?

EPR introduce a general pure state held by (say) Alice and Bob:

$$|\Psi\rangle = \sum_{n=1}^{\infty} c_n |u_n\rangle|\psi_n\rangle = \sum_{s=1}^{\infty} d_s |v_s\rangle|\varphi_s\rangle. \quad (1)$$

If Alice measures in the $\{|u_n\rangle\}$ (resp. $\{|v_s\rangle\}$) basis, she would instantly collapse Bob's system into one of the states $|\psi_n\rangle$ (resp. $|\varphi_s\rangle$):

> *[A]s a consequence of two different measurements performed upon the first system, the* [distant] *second system may be left in states with two different* [types of] *wavefunctions.*

- Schrödinger (1935) called this **steering** or **piloting** the remote state, and generalized it to arbitrarily many measurements by Alice.

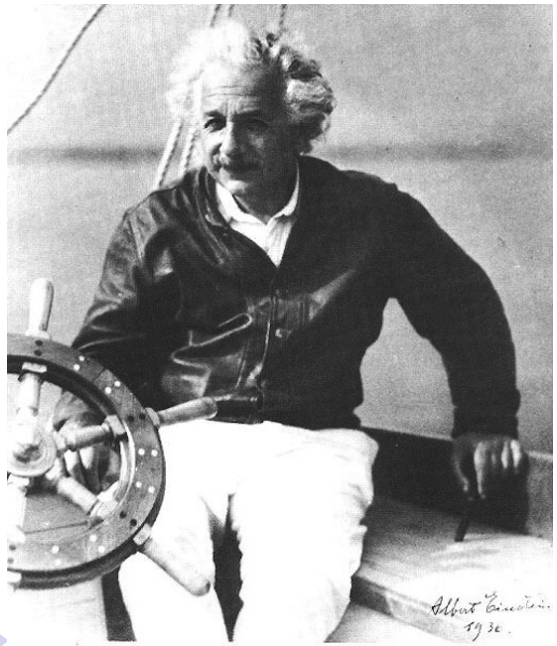
Why EPR-*Steering*?

EPR introduce a general pure state held by (say) Alice and Bob:

$$|\Psi\rangle = \sum_{n=1}^{\infty} c_n |u_n\rangle|\psi_n\rangle = \sum_{s=1}^{\infty} d_s |v_s\rangle|\varphi_s\rangle. \quad (1)$$

If Alice measures in the $\{|u_n\rangle\}$ (resp. $\{|v_s\rangle\}$) basis, she would instantly collapse Bob's system into one of the states $|\psi_n\rangle$ (resp. $|\varphi_s\rangle$):

> *[A]s a consequence of two different measurements performed upon the first system, the* [distant] *second system may be left in states with two different* [types of] *wavefunctions.*



- Schrödinger (1935) called this **steering** or **piloting** the remote state, and generalized it to arbitrarily many measurements by Alice.

Formalizing EPR-Steering, 2007

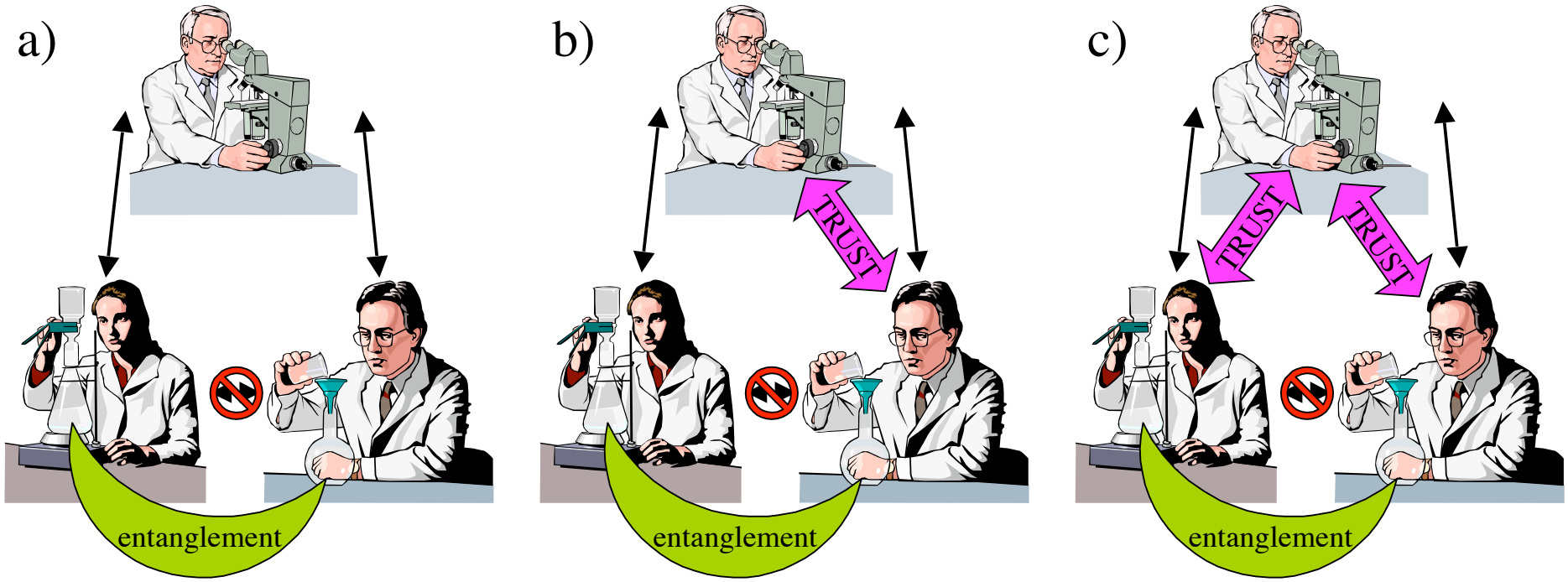
- HMW, Jones & Doherty (PRL, 2007) formalized and generalized EPR-steering: to demonstrate EPR-steering is to demonstrate that a **Local Hidden State** assumption for Bob cannot hold.
- The LHS assumption is that Bob has a local hidden state $|\phi_\xi\rangle$ (hidden to him, but perhaps known to Alice) with probability $\wp_\xi$.
- No assumptions at all are made about Alice, except that, being distant, she cannot alter Bob's state.
- That is, different measurements for Alice can only mean different processing of her potential information (ξ).
- In analogy with Bell inequalities, one can construct EPR-steering inequalities (bipartite correlation functions), the violation of which demonstrates the failure of the LHS assumption.

Formalizing EPR-Steering, 2007

- HMW, Jones & Doherty (PRL, 2007) formalized and generalized EPR-steering: to demonstrate EPR-steering is to demonstrate that a **Local Hidden State** assumption for Bob cannot hold.
- The LHS assumption is that Bob has a local hidden state $|\phi_\xi\rangle$ (hidden to him, but perhaps known to Alice) with probability $\wp_\xi$.
- No assumptions at all are made about Alice, except that, being distant, she cannot alter Bob's state.
- That is, different measurements for Alice can only mean different processing of her potential information (ξ).
- In analogy with Bell inequalities, one can construct EPR-steering inequalities (bipartite correlation functions), the violation of which demonstrates the failure of the LHS assumption.

Quantum Information Approach

Consider a quantum information lab with PhD student Alice, Postdoc Bob, and Professor Charlie. Charlie wants proof that Alice and Bob can create a shared entangled state. There are three cases to consider:



Black arrows show classical communication, forbidden between Alice & Bob.

Bell nonlolocality $\Longrightarrow$ **EPR-steering** $\Longrightarrow$ **entanglement.**

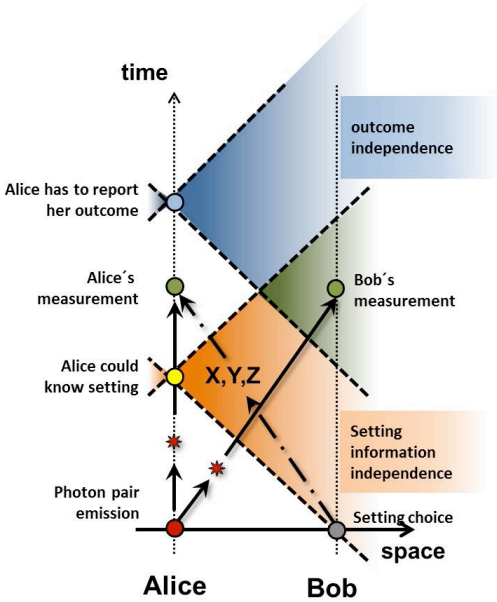
Loop-hole-free EPR-Steering

- Entanglement witnessing has no loopholes ∴ Alice & Bob are trusted.
- Bell-nonlocality has the three well-known loopholes: *efficiency*, *freedom of choice*, and *separation*.
- EPR-steering has the same loopholes, but asymmetrically. We need *efficiency for Alice*, *freedom of choice for Bob*, and *separation*.
- Still only one experiment that closes all the loopholes (2012):

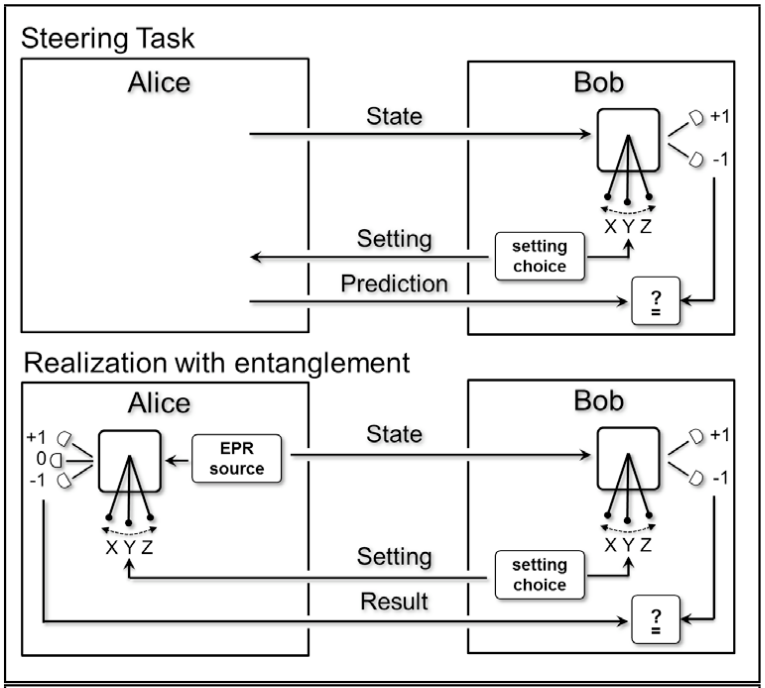
New Journal of Physics
The open-access journal for physics

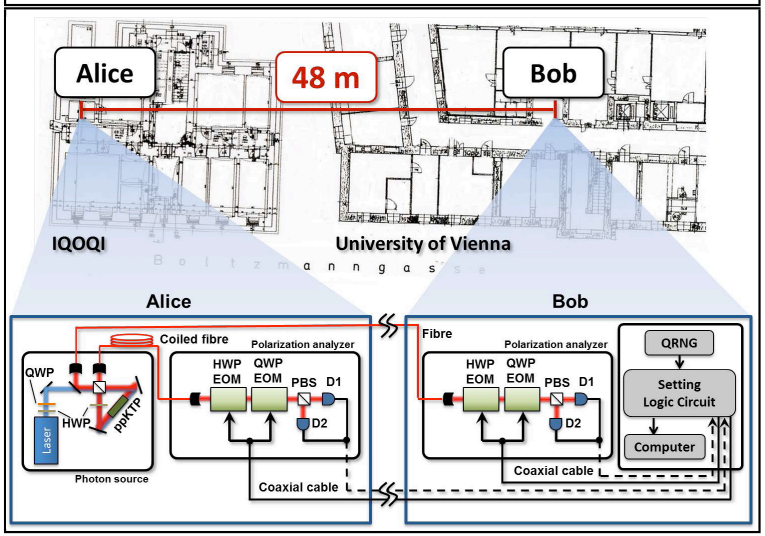
Loophole-free Einstein–Podolsky–Rosen experiment via quantum steering

Bernhard Wittmann[1,2,6,7], Sven Ramelow[1,2,6,7], Fabian Steinlechner[2], Nathan K Langford[2], Nicolas Brunner[3], Howard M Wiseman[4], Rupert Ursin[2] and Anton Zeilinger[1,2,5]



Closing the Loopholes





To demonstrate EPR-steering we violate the LHS prediction

$$S \equiv T_X + T_Y + T_Z \leq 1,$$

where

$$T_X = \mathrm{E}^{A_X} \left\{ \left(\langle \hat{\sigma}_x^{\mathrm{Bob}} \rangle_j^{A_X} \right)^2 \right\}.$$

where the ensemble average E^{A_X} is the average over Alice's result $j \in \{-1, \emptyset, 1\}$ when she measures X.

Experimentally we observed

$$S = 1.049 \pm 0.002 > 1.$$

Outline

Quantum State Confusion (1992)

When I began my PhD there were (at least) four schools of thought:

- There are **no quantum jumps**. The atom's state is described by a density operator or *state matrix* ρ which evolves smoothly under the master equation $\dot{\rho} = \mathcal{L}\rho$.
- There are measurement-induced quantum jumps in which the atom collapses to the ground state at the (retarded) time at which a **photon is detected**. e.g. Cohen-Tannoudji
- There are quantum jumps but they occur regardless of whether there is any photon detection; they are caused by randomly occurring **photon emission** as in the Old Quantum Theory.
- Maybe there are no quantum jumps but rather an individual atom undergoes **quantum state diffusion**. e.g. Gisin & Percival (1992)

The Modern Understanding: Open Quantum Systems

- Open = continuously coupled to an environment or *bath*.
- This creates entanglement between the system and environment.
- If we ignore the bath then even if both system and bath are initially pure, the system state will decohere:

$$|\Psi(0)\rangle = |\phi(0)\rangle_{\rm env} \otimes |\psi(0)\rangle_{\rm sys} \rightarrow |\Psi(t)\rangle = \exp\left(-i\hat{H}_{\rm tot}t\right)|\Psi(0)\rangle$$

$$\text{(pure) } |\psi(0)\rangle_{\rm sys} \rightarrow \rho_{\rm sys}(t) = {\rm Tr}_{\rm env}[|\Psi(t)\rangle\langle\Psi(t)|] \text{ (mixed)}$$

- For many atomic, optical, and (increasingly) solid-state systems, this can be described by a Markovian quantum master equation (of the Lindblad form):

$$\dot{\rho}(t) = \mathcal{L}\rho(t) \equiv [-i\hat{H},\rho] + \sum_{l=1}^{L} \hat{c}_l \rho \hat{c}_l^\dagger - \tfrac{1}{2}\{\hat{c}_l^\dagger \hat{c}_l, \rho\}.$$

Unravelling Quantum Master Equations

- It is not always appropriate to ignore the bath — often it can be measured, yielding information about the system.
- *If* a Markovian master equation can be derived
  then
  the bath can be measured repeatedly (monitored), on a time scale which is short compared to the interesting system evolution, *without invalidating the master equation*.
- For perfect monitoring the conditioned system state is *pure* $|\psi_j(t)\rangle$.
- Carmichael (1993) called this *unravelling* the ME into an ensemble of **stochastic** *quantum trajectories* for $|\psi_j(t)\rangle$:

$$\mathrm{E}[|\psi_j(t)\rangle\langle\psi_j(t)|] = \rho(t) = \exp(\mathcal{L}t)|\psi(0)\rangle\langle\psi(0)|.$$

- e.g. monitoring the bath photon-number causes the system to undergo a *quantum jump* when a new photon is detected.

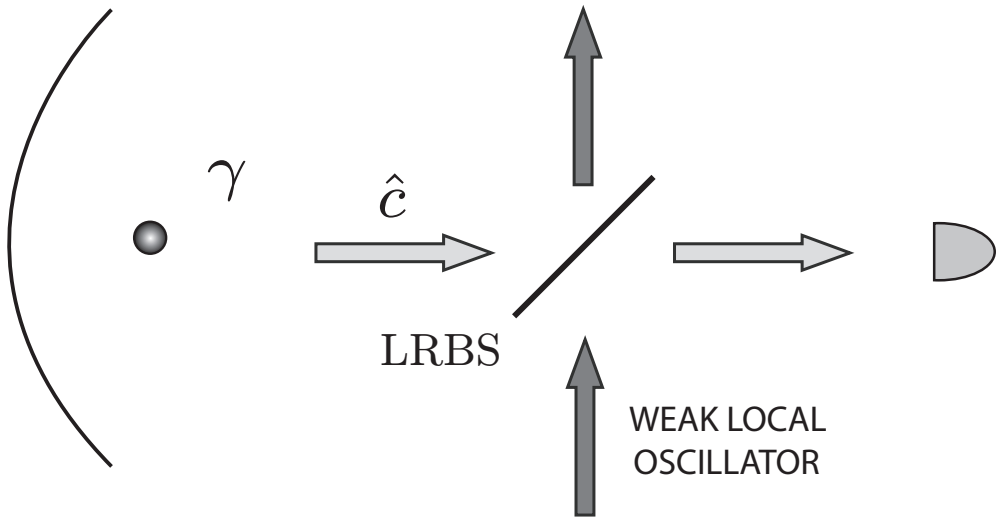
Detection, or Emission — Who Cares?

- If there were only one way to detect a field, no-one should care.
- But there isn't. For an atom (or any Markovian system) the average system dynamics $\dot{\rho} = \mathcal{L}\rho$ is unchanged by any processing of the system output fields prior to detection.
- e.g. we can add a local oscillator field β.
- Mathematically, this amounts to $\hat{c} \to \hat{c} + \beta$, $\hat{H} \to \hat{H} - \frac{i}{2}(\beta^* \hat{c} - \beta \hat{c}^\dagger)$.
- We can even do this *adaptively*, making $\beta(t)$ depend on prior clicks.

Detection, or Emission — Who Cares?

- If there were only one way to detect a field, no-one should care.
- But there isn't. For an atom (or any Markovian system) the average system dynamics $\dot{\rho} = \mathcal{L}\rho$ is unchanged by any processing of the system output fields prior to detection.

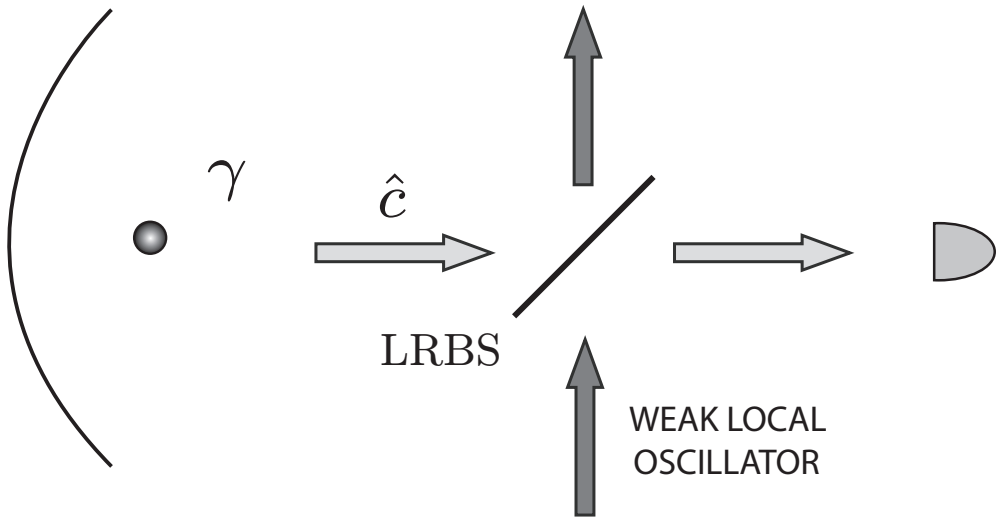
- e.g. we can add a local oscillator field β.
- Mathematically, this amounts to $\hat{c} \to \hat{c} + \beta$, $\hat{H} \to \hat{H} - \frac{i}{2}(\beta^* \hat{c} - \beta \hat{c}^\dagger)$.
- We can even do this *adaptively*, making $\beta(t)$ depend on prior clicks.



Detection, or Emission — Who Cares?

- If there were only one way to detect a field, no-one should care.
- But there isn't. For an atom (or any Markovian system) the average system dynamics $\dot{\rho} = \mathcal{L}\rho$ is unchanged by any processing of the system output fields prior to detection.

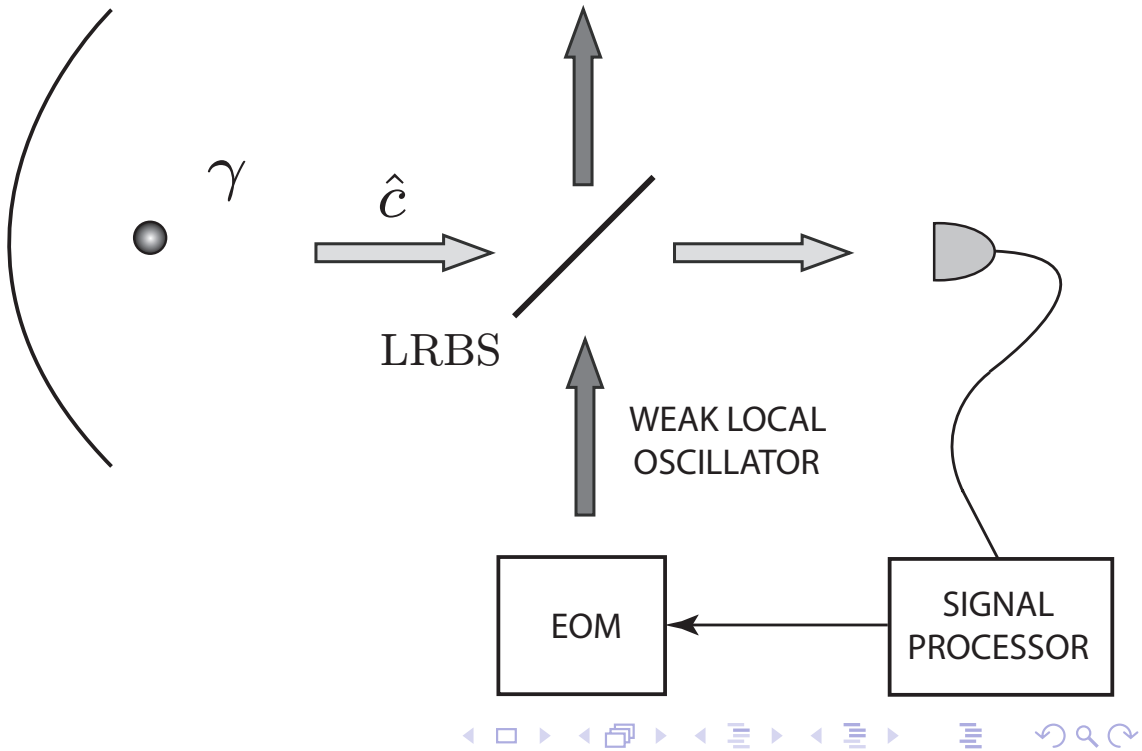
- e.g. we can add a local oscillator field β.
- Mathematically, this amounts to $\hat{c} \to \hat{c} + \beta$, $\hat{H} \to \hat{H} - \frac{i}{2}(\beta^* \hat{c} - \beta \hat{c}^\dagger)$.
- We can even do this *adaptively*, making $\beta(t)$ depend on prior clicks.



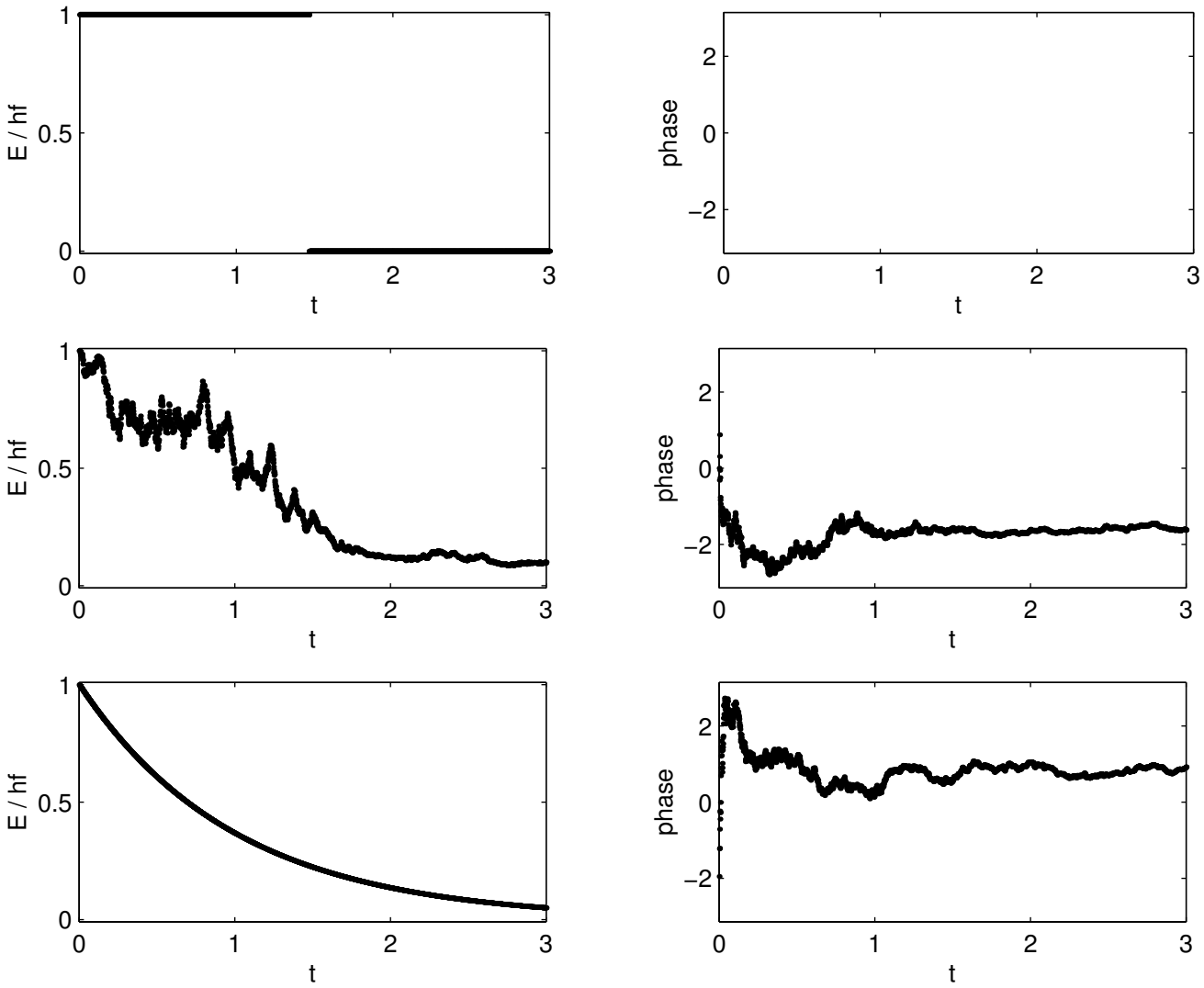
Detection, or Emission — Who Cares?

- If there were only one way to detect a field, no-one should care.
- But there isn't. For an atom (or any Markovian system) the average system dynamics $\dot{\rho} = \mathcal{L}\rho$ is unchanged by any processing of the system output fields prior to detection.

- e.g. we can add a local oscillator field β.
- Mathematically, this amounts to $\hat{c} \to \hat{c} + \beta$, $\hat{H} \to \hat{H} - \frac{i}{2}(\beta^* \hat{c} - \beta \hat{c}^\dagger)$.
- We can even do this *adaptively*, making $\beta(t)$ depend on prior clicks.

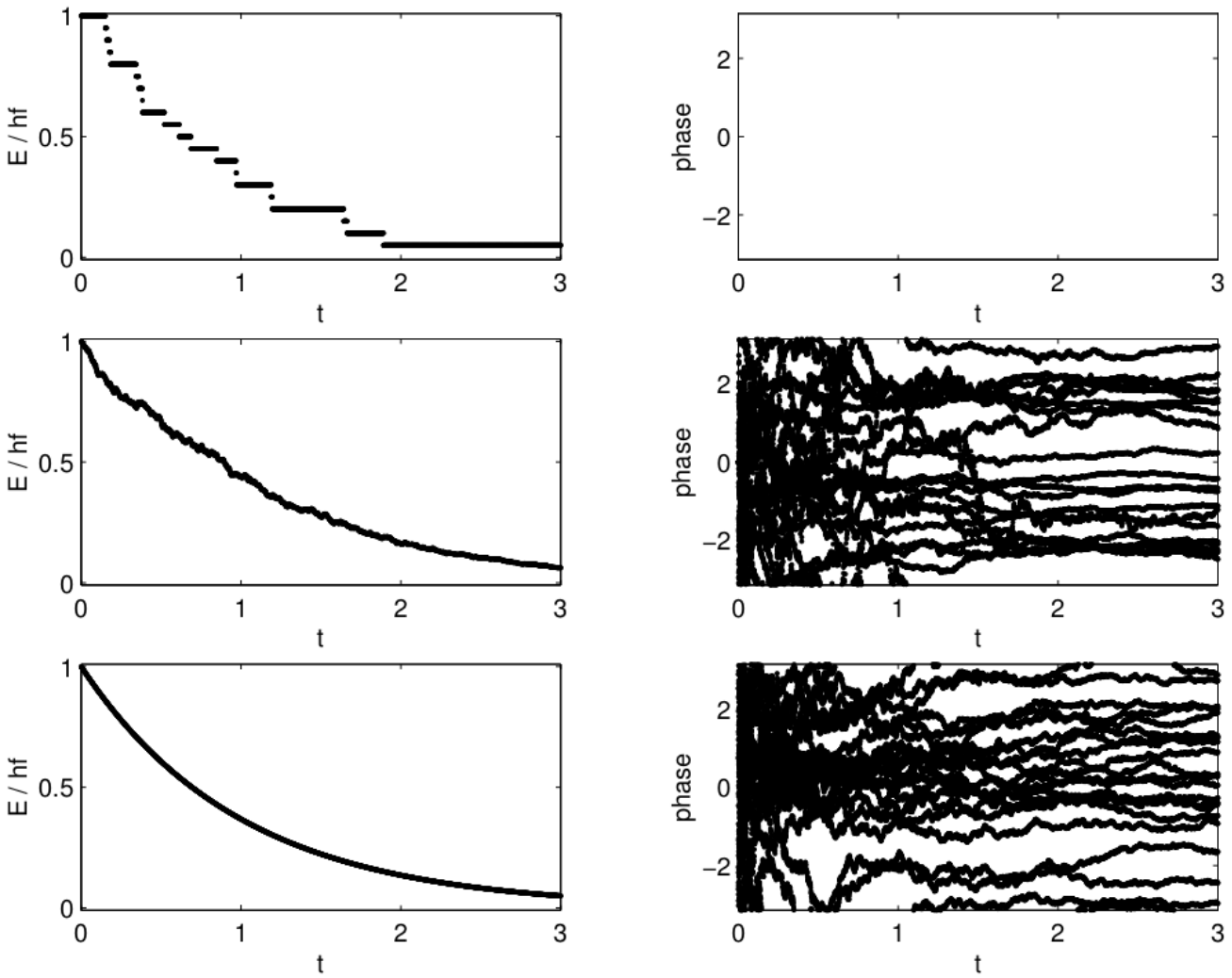


Example: Stochastic Decay of Excited State Atom



- Direct Detection.
- QSD (1992) = Heterodyne Detection (HMW & GJM, 1993).
- Adaptive Homodyne Detection (HMW, 1995).

Example: Ensemble Average Decay



- Direct Detection.
- QSD (1992) = Heterodyne Detection (HMW & GJM, 1993).
- Adaptive Homodyne Detection (HMW, 1995).

Are dynamical quantum jumps detector-dependent?

- Yes!
- In theory.
- But has the theory ever been tested?
- Can we be sure that a two-level atom does not actually
  - Emit a photon and jump to the ground state as in Bohr's model?
  - Undergo Quantum State Diffusion (QSD), the detector-independent model introduced by Gisin and Percival in 1992?
  - Undergo stochastic evolution according to some other *objective pure-state dynamical model* (OPDM)?

Question

Can we derive **realistic** *experimental tests that would rule out* **all** *OPDMs, including objective quantum jumps, and QSD?*

- **Realistic** means not assuming efficient detection.
- We also want to avoid any special preparation of the atom or field.

Are dynamical quantum jumps detector-dependent?

- Yes!
- In theory.
- But has the theory ever been tested?
- Can we be sure that a two-level atom does not actually
  - Emit a photon and jump to the ground state as in Bohr's model?
  - Undergo Quantum State Diffusion (QSD), the detector-independent model introduced by Gisin and Percival in 1992?
  - Undergo stochastic evolution according to some other *objective pure-state dynamical model* (OPDM)?

Question

Can we derive **realistic** *experimental tests that would rule out* **all** *OPDMs, including objective quantum jumps, and QSD?*

- **Realistic** means not assuming efficient detection.
- We also want to avoid any special preparation of the atom or field.

Are dynamical quantum jumps detector-dependent?

- Yes!
- In theory.
- But has the theory ever been tested?
- Can we be sure that a two-level atom does not actually
  - Emit a photon and jump to the ground state as in Bohr's model?
  - Undergo Quantum State Diffusion (QSD), the detector-independent model introduced by Gisin and Percival in 1992?
  - Undergo stochastic evolution according to some other *objective pure-state dynamical model* (OPDM)?

Question

Can we derive **realistic** *experimental tests that would rule out* **all** *OPDMs, including objective quantum jumps, and QSD?*

- **Realistic** means not assuming efficient detection.
- We also want to avoid any special preparation of the atom or field.

Are dynamical quantum jumps detector-dependent?

- Yes!
- In theory.
- But has the theory ever been tested?
- Can we be sure that a two-level atom does not actually
  - Emit a photon and jump to the ground state as in Bohr's model?
  - Undergo Quantum State Diffusion (QSD), the detector-independent model introduced by Gisin and Percival in 1992?
  - Undergo stochastic evolution according to some other *objective pure-state dynamical model* (OPDM)?

Question

Can we derive **realistic** *experimental tests that would rule out* **all** *OPDMs, including objective quantum jumps, and QSD?*

- **Realistic** means not assuming efficient detection.
- We also want to avoid any special preparation of the atom or field.

Are dynamical quantum jumps detector-dependent?

- Yes!
- In theory.
- But has the theory ever been tested?
- Can we be sure that a two-level atom does not actually
  - Emit a photon and jump to the ground state as in Bohr's model?
  - Undergo Quantum State Diffusion (QSD), the detector-independent model introduced by Gisin and Percival in 1992?
  - Undergo stochastic evolution according to some other *objective pure-state dynamical model* (OPDM)?

Question

Can we derive **realistic** *experimental tests that would rule out* **all** *OPDMs, including objective quantum jumps, and QSD?*

- **Realistic** means not assuming efficient detection.
- We also want to avoid any special preparation of the atom or field.

Are dynamical quantum jumps detector-dependent?

- Yes!
- In theory.
- But has the theory ever been tested?
- Can we be sure that a two-level atom does not actually
  - Emit a photon and jump to the ground state as in Bohr's model?
  - Undergo Quantum State Diffusion (QSD), the detector-independent model introduced by Gisin and Percival in 1992?
  - Undergo stochastic evolution according to some other *objective pure-state dynamical model* (OPDM)?

Question

Can we derive **realistic** *experimental tests that would rule out* **all** *OPDMs, including objective quantum jumps, and QSD?*

- **Realistic** means not assuming efficient detection.
- We also want to avoid any special preparation of the atom or field.

2-setting EPR-steering Inequality for a Qubit

- If Bob has a qubit (2LA) then for any $|\phi\rangle$, $\langle\hat{\sigma}_x\rangle^2 + \langle\hat{\sigma}_y\rangle^2 + \langle\hat{\sigma}_z\rangle^2 \leq 1$.
- Say that Alice can perform two different measurements A_1 and A_2.
- Then under the LHS assumption it follows that (for example),

$$S \equiv \mathrm{E}^{A_1}\left\{\left(\langle\hat{\sigma}_x\rangle_j^{A_1}\right)^2\right\} + \mathrm{E}^{A_2}\left\{\left(\langle\hat{\sigma}_y\rangle_j^{A_2}\right)^2 + \left(\langle\hat{\sigma}_z\rangle_j^{A_2}\right)^2\right\} \leq 1.$$

where j (Alice's "result") is the index for the ensemble, so

$$\text{e.g. } \mathrm{E}^{A_1}\left\{\left(\langle\hat{\sigma}_x\rangle_j^{A_1}\right)^2\right\} \equiv \sum_j \wp_j^{A_1}\left(\mathrm{Tr}\left[\rho_j^{A_1}\hat{\sigma}_x\right]\right)^2$$

is an average property of Bob's state conditioned on Alice's j.

- If this inequality is violated, that demonstrates EPR-steering.

EPR-steering for a continuously monitored system

- If Bob's atom evolved according to an objective pure-state dynamical model (OPSDM) then at all times t it would be in some pure state $|\phi_\xi\rangle$, and Alice's best knowledge would be if she knew ξ.
- We can disprove every OPSDM if Alice can implement two different monitoring schemes on the atom's fluorescence, A_1 and A_2, which allow her to violate an EPR-steering inequality.
- Waiting until **steady-state** allows time for entanglement to grow.
- Thus to test the EPR-steering inequality Bob should:
  1. Randomly choose $\alpha = 1$ or 2, and tell Alice to implement A_1 or A_2.
  2. Randomly choose the time t ($\gg$ the system relaxation time) and measure $\hat{\sigma}_x$ or $\hat{\sigma}_y$ or $\hat{\sigma}_z$ at this time.
  3. Ask Alice which state (from a set $\{\rho_j^{A_\alpha}\}$ nominated earlier by her) pertained to his atom at time t.
  4. Store his data in different files for different α and j.

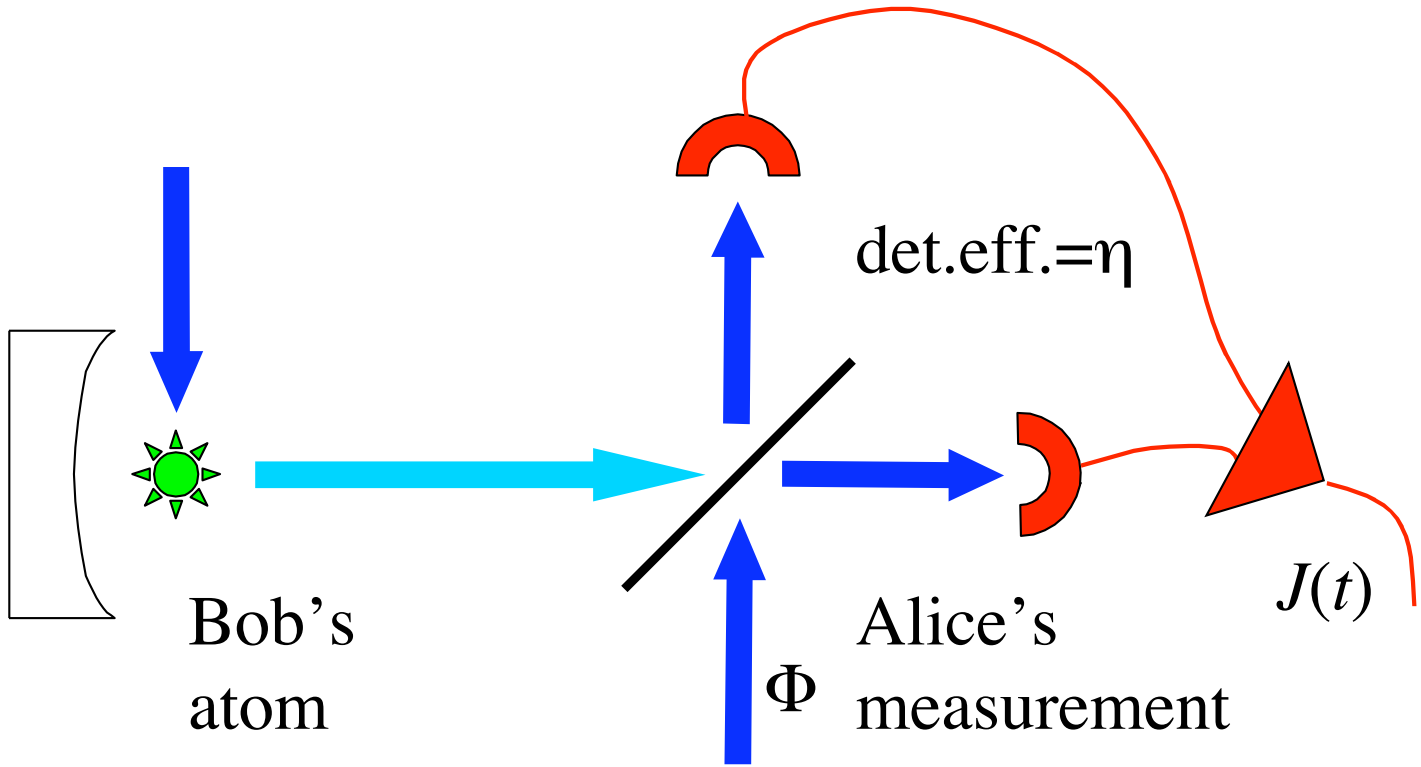
EPR-steering for a continuously monitored system

- If Bob's atom evolved according to an objective pure-state dynamical model (OPSDM) then at all times t it would be in some pure state $|\phi_\xi\rangle$, and Alice's best knowledge would be if she knew ξ.
- We can disprove every OPSDM if Alice can implement two different monitoring schemes on the atom's fluorescence, A_1 and A_2, which allow her to violate an EPR-steering inequality.
- Waiting until **steady-state** allows time for entanglement to grow.
- Thus to test the EPR-steering inequality Bob should:

1. Randomly choose $\alpha = 1$ or 2, and tell Alice to implement A_1 or A_2.
2. Randomly choose the time t ($\gg$ the system relaxation time) and measure $\hat{\sigma}_x$ or $\hat{\sigma}_y$ or $\hat{\sigma}_z$ at this time.
3. Ask Alice which state (from a set $\{\rho_j^{A_\alpha}\}$ nominated earlier by her) pertained to his atom at time t.
4. Store his data in different files for different α and j.

What types of monitoring schemes?

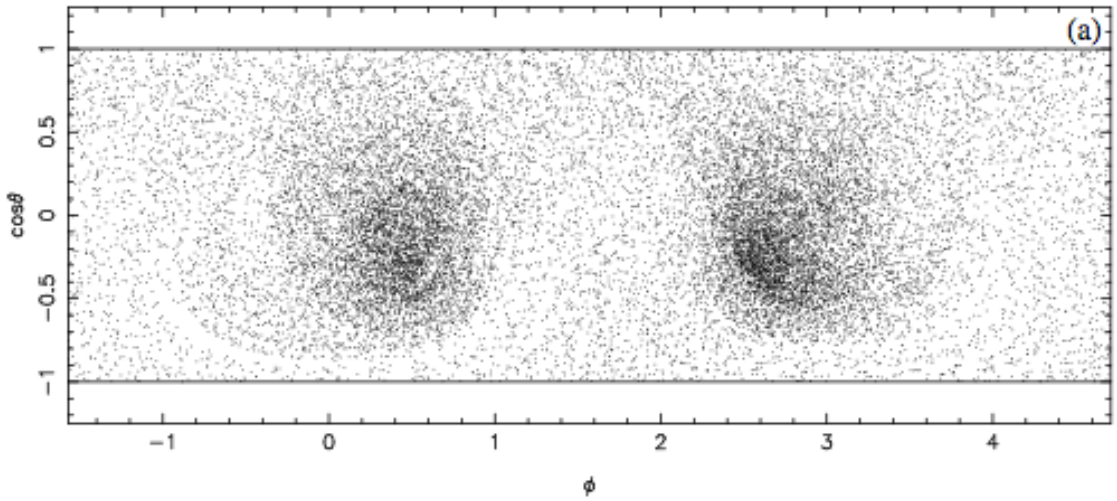
- Presently, the best efficiency is with homodyne measurement.
- This uses a strong local oscillator with a **choice of phase** Φ.



- The index j defining the state $\rho_j^{A_\alpha}$ will depend on the complete photocurrent record $J^\alpha(s)$ for $0 \leq s < t$.

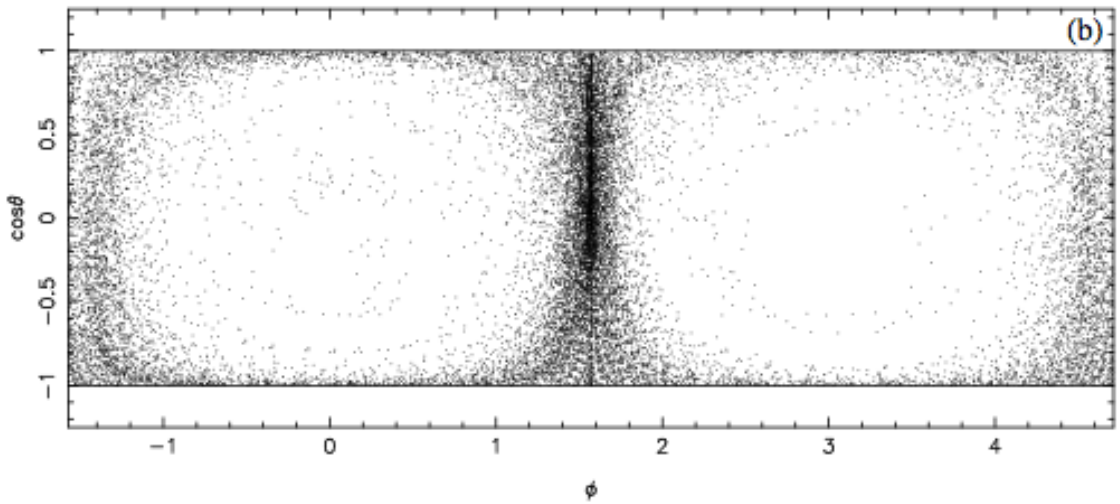
Homodyne *x* versus Homodyne *y*

In the strong driving limit ($\hat{H} = \frac{\Omega}{2}\hat{\sigma}_x; \Omega \gtrsim \gamma$) these two monitorings with $\eta = 1$ should give distinctly different atomic-state trajectories:



A_1: homo-x ($\Phi = 0$).

ρ_j *tends* to localize at longitude $\phi = 0$ or $\phi = \pi$, near the states: $\langle\hat{\sigma}_x\rangle = \pm 1$.



A_2: homo-y ($\Phi = \frac{\pi}{2}$).

ρ_j is confined to the $\hat{\sigma}_x = 0$ great circle ($\phi = \pm\pi/2$) where $\langle\hat{\sigma}_y\rangle^2 + \langle\hat{\sigma}_z\rangle^2 = 1$.

Applying the Steering Inequality[1]

Recall: LHS $\implies$ $S \equiv \mathrm{E}^{A_1}\left\{\left(\langle\hat{\sigma}_x\rangle_j^{A_1}\right)^2\right\} + \mathrm{E}^{A_2}\left\{\left(\langle\hat{\sigma}_y\rangle_j^{A_2}\right)^2 + \left(\langle\hat{\sigma}_z\rangle_j^{A_2}\right)^2\right\} \leq 1.$

The above behaviours of the 2LA under unravellings A_1 (homo-x) and A_2 (homo-y) suggest this is a good inequality to try to violate.

As a function of η (assumed the same for A_1 and A_2), we need a *total* efficiency $\eta > 73\%$.

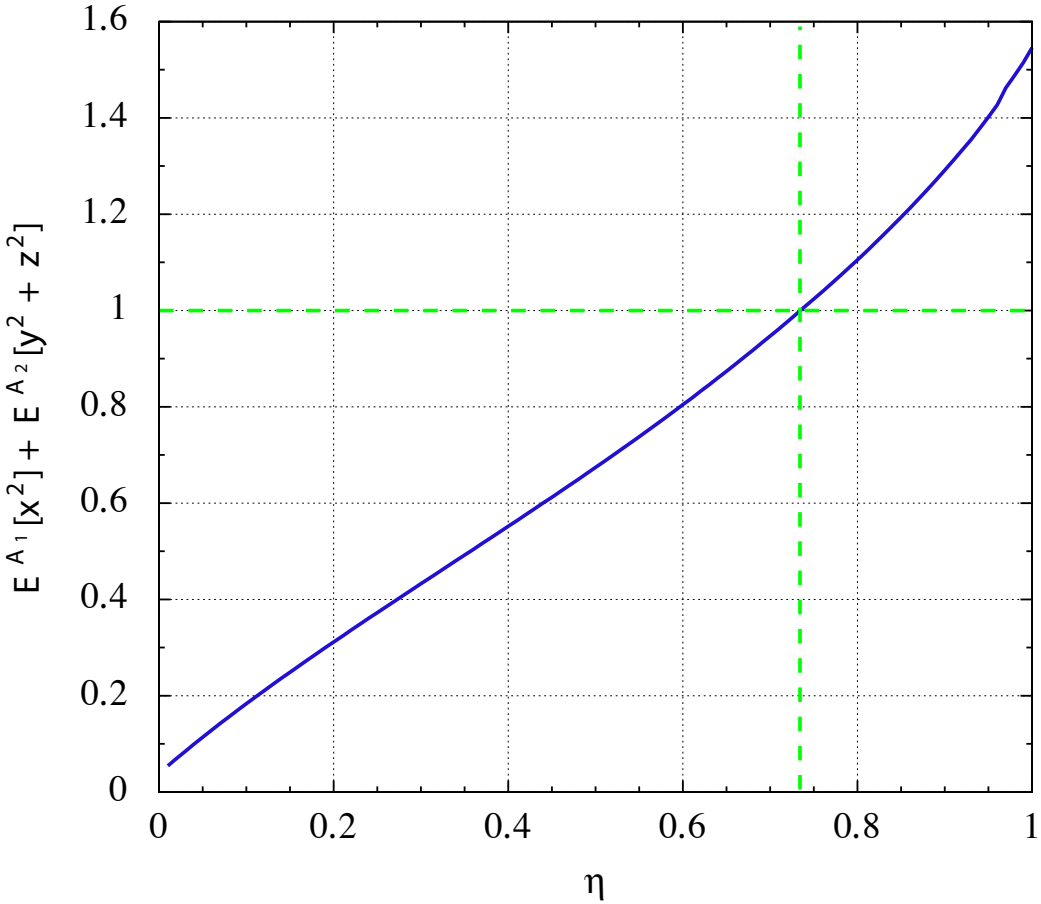
[1] H. M. Wiseman & Jay M. Gambetta, Phys. Rev. Lett. **108**, 220402 (2012).

Applying the Steering Inequality[1]

Recall: LHS $\implies$ $S \equiv \mathrm{E}^{A_1}\left\{\left(\langle\hat{\sigma}_x\rangle_j^{A_1}\right)^2\right\} + \mathrm{E}^{A_2}\left\{\left(\langle\hat{\sigma}_y\rangle_j^{A_2}\right)^2 + \left(\langle\hat{\sigma}_z\rangle_j^{A_2}\right)^2\right\} \leq 1.$

The above behaviours of the 2LA under unravellings A_1 (homo-x) and A_2 (homo-y) suggest this is a good inequality to try to violate.

As a function of η (assumed the same for A_1 and A_2), we need a *total* efficiency $\eta > 73\%$.



[1] H. M. Wiseman & Jay M. Gambetta, Phys. Rev. Lett. **108**, 220402 (2012).

Can we do better?

- By considering **non-homodyne schemes**, Yes!
- To maximize $\mathrm{E}^{A_2}\{(\langle\hat{\sigma}_y\rangle_j^{A_2})^2+(\langle\hat{\sigma}_z\rangle_j^{A_2})^2\}$, y-homodyne seems best.
- But to maximize $\mathrm{E}^{A_1}\{(\langle\hat{\sigma}_x\rangle_j^{A_1})^2\}$, in the limit $\Omega \gg \gamma$, scheme 's' — a spectrally-resolving scheme (invented by us) using an adaptively controlled weak local oscillator — is better than homodyne x.
- For equal efficiencies, the threshold is then 58%, much closer to the two-measurement minimum of $\eta > 0.5$.
- What about **more than two different homodyne schemes** e.g. $\Phi = 0$, $\Phi = \pi/2$, $\Phi = \pi/4$ ... ?
- We have shown that *for any quantum system* with a single decay channel, **no matter** how many different homodyne (and heterodyne etc.) schemes are implemented it is **impossible** to demonstrate EPR-steering unless $\eta > 0.5$.
- So $\eta > 0.73$ for two homodyne schemes is not bad.

Can we do better?

- By considering **non-homodyne schemes**, Yes!
- To maximize $\mathrm{E}^{A_2}\{(\langle\hat{\sigma}_y\rangle_j^{A_2})^2+(\langle\hat{\sigma}_z\rangle_j^{A_2})^2\}$, y-homodyne seems best.
- But to maximize $\mathrm{E}^{A_1}\{(\langle\hat{\sigma}_x\rangle_j^{A_1})^2\}$, in the limit $\Omega \gg \gamma$, scheme 's' — a spectrally-resolving scheme (invented by us) using an adaptively controlled weak local oscillator — is better than homodyne x.
- For equal efficiencies, the threshold is then 58%, much closer to the two-measurement minimum of $\eta > 0.5$.
- What about **more than two different homodyne schemes** e.g. $\Phi = 0$, $\Phi = \pi/2$, $\Phi = \pi/4$ ... ?
- We have shown that *for any quantum system* with a single decay channel, **no matter** how many different homodyne (and heterodyne etc.) schemes are implemented it is **impossible** to demonstrate EPR-steering unless $\eta > 0.5$.
- So $\eta > 0.73$ for two homodyne schemes is not bad.

Can we do better?

- By considering **non-homodyne schemes**, Yes!
- To maximize $\mathrm{E}^{A_2}\{(\langle\hat{\sigma}_y\rangle_j^{A_2})^2+(\langle\hat{\sigma}_z\rangle_j^{A_2})^2\}$, y-homodyne seems best.
- But to maximize $\mathrm{E}^{A_1}\{(\langle\hat{\sigma}_x\rangle_j^{A_1})^2\}$, in the limit $\Omega \gg \gamma$, scheme 's' — a spectrally-resolving scheme (invented by us) using an adaptively controlled weak local oscillator — is better than homodyne x.
- For equal efficiencies, the threshold is then 58%, much closer to the two-measurement minimum of $\eta > 0.5$.
- What about **more than two different homodyne schemes** e.g. $\Phi = 0$, $\Phi = \pi/2$, $\Phi = \pi/4$ ... ?
- We have shown that *for any quantum system* with a single decay channel, **no matter** how many different homodyne (and heterodyne etc.) schemes are implemented it is **impossible** to demonstrate EPR-steering unless $\eta > 0.5$.
- So $\eta > 0.73$ for two homodyne schemes is not bad.

Can we do better?

- By considering **non-homodyne schemes**, Yes!
- To maximize $\mathrm{E}^{A_2}\{(\langle\hat{\sigma}_y\rangle_j^{A_2})^2+(\langle\hat{\sigma}_z\rangle_j^{A_2})^2\}$, y-homodyne seems best.
- But to maximize $\mathrm{E}^{A_1}\{(\langle\hat{\sigma}_x\rangle_j^{A_1})^2\}$, in the limit $\Omega \gg \gamma$, scheme 's' — a spectrally-resolving scheme (invented by us) using an adaptively controlled weak local oscillator — is better than homodyne x.
- For equal efficiencies, the threshold is then 58%, much closer to the two-measurement minimum of $\eta > 0.5$.
- What about **more than two different homodyne schemes** e.g. $\Phi = 0$, $\Phi = \pi/2$, $\Phi = \pi/4$ ... ?
- We have shown that *for any quantum system* with a single decay channel, **no matter** how many different homodyne (and heterodyne etc.) schemes are implemented it is **impossible** to demonstrate EPR-steering unless $\eta > 0.5$.
- So $\eta > 0.73$ for two homodyne schemes is not bad.

Can we do better?

- By considering **non-homodyne schemes**, Yes!
- To maximize $\mathrm{E}^{A_2}\{(\langle\hat{\sigma}_y\rangle_j^{A_2})^2+(\langle\hat{\sigma}_z\rangle_j^{A_2})^2\}$, y-homodyne seems best.
- But to maximize $\mathrm{E}^{A_1}\{(\langle\hat{\sigma}_x\rangle_j^{A_1})^2\}$, in the limit $\Omega \gg \gamma$, scheme 's' — a spectrally-resolving scheme (invented by us) using an adaptively controlled weak local oscillator — is better than homodyne x.
- For equal efficiencies, the threshold is then 58%, much closer to the two-measurement minimum of $\eta > 0.5$.
- What about **more than two different homodyne schemes** e.g. $\Phi = 0$, $\Phi = \pi/2$, $\Phi = \pi/4$ ... ?
- We have shown that *for any quantum system* with a single decay channel, **no matter** how many different homodyne (and heterodyne etc.) schemes are implemented it is **impossible** to demonstrate EPR-steering unless $\eta > 0.5$.
- So $\eta > 0.73$ for two homodyne schemes is not bad.

Outline

Standard Quantum Key Distribution

- Enables distant parties (Alice & Bob) to establish a *key* (a shared string of random bits), guaranteed unknown to any eavesdropper.
- The key can then be used by Alice to encode a message for Bob.
- Standard protocol is *prepare and measure* (P&M):
  1. Alice sends a sequence of qubits, each randomly prepared in one of 4 states: $|\uparrow\rangle$, $|\downarrow\rangle$, $|\rightarrow\rangle$, $|\leftarrow\rangle$ with unambiguity μ_A.
  2. Bob randomly measures in basis Z ($\updownarrow$) or X ($\leftrightarrow$) with efficiency η_B.
  3. Bob publicly reveals which basis in each case, and Alice publicly reveals for which of these she could hope to predict Bob's answer.
  4. They publicly determine the error rate $Q^{\rm ps}$ [2] in a randomly chosen subset of these cases, which enables them to *lower bound* how much information the eavesdropper Eve may have.
  5. If Q is low enough, they can extract (by public communication) from $n \gg 1$ qubits a key of length $\ell > \eta_B \mu_A [1 - h(Q_X^{\rm ps}) - h(Q_Z^{\rm ps})]n$.
- We call $r = \eta_B \mu_A [1 - h(Q_X^{\rm ps}) - h(Q_Z^{\rm ps})]$ the *key rate*.

[2] post-selected on unambiguous qubit preparation by Alice and detection by Bob.

Standard Quantum Key Distribution

- Enables distant parties (Alice & Bob) to establish a *key* (a shared string of random bits), guaranteed unknown to any eavesdropper.
- The key can then be used by Alice to encode a message for Bob.
- Standard protocol is *prepare and measure* (P&M):
  1. Alice sends a sequence of qubits, each randomly prepared in one of 4 states: $|\uparrow\rangle$, $|\downarrow\rangle$, $|\rightarrow\rangle$, $|\leftarrow\rangle$ with unambiguity μ_A.
  2. Bob randomly measures in basis Z ($\updownarrow$) or X ($\leftrightarrow$) with efficiency η_B.
  3. Bob publicly reveals which basis in each case, and Alice publicly reveals for which of these she could hope to predict Bob's answer.
  4. They publicly determine the error rate $Q^{\rm ps}$ [2] in a randomly chosen subset of these cases, which enables them to *lower bound* how much information the eavesdropper Eve may have.
  5. If Q is low enough, they can extract (by public communication) from $n \gg 1$ qubits a key of length $\ell > \eta_B \mu_A [1 - h(Q_X^{\rm ps}) - h(Q_Z^{\rm ps})]n$.
- We call $r = \eta_B \mu_A [1 - h(Q_X^{\rm ps}) - h(Q_Z^{\rm ps})]$ the *key rate*.

[2] post-selected on unambiguous qubit preparation by Alice and detection by Bob.

Standard Quantum Key Distribution

- Enables distant parties (Alice & Bob) to establish a *key* (a shared string of random bits), guaranteed unknown to any eavesdropper.
- The key can then be used by Alice to encode a message for Bob.
- Standard protocol is *prepare and measure* (P&M):
  1. Alice sends a sequence of qubits, each randomly prepared in one of 4 states: $|\uparrow\rangle$, $|\downarrow\rangle$, $|\rightarrow\rangle$, $|\leftarrow\rangle$ with unambiguity μ_A.
  2. Bob randomly measures in basis Z ($\updownarrow$) or X ($\leftrightarrow$) with efficiency η_B.
  3. Bob publicly reveals which basis in each case, and Alice publicly reveals for which of these she could hope to predict Bob's answer.
  4. They publicly determine the error rate $Q^{\rm ps}$ [2] in a randomly chosen subset of these cases, which enables them to *lower bound* how much information the eavesdropper Eve may have.
  5. If Q is low enough, they can extract (by public communication) from $n \gg 1$ qubits a key of length $\ell > \eta_B\mu_A[1 - h(Q_X^{\rm ps}) - h(Q_Z^{\rm ps})]n$.
- We call $r = \eta_B\mu_A[1 - h(Q_X^{\rm ps}) - h(Q_Z^{\rm ps})]$ the *key rate*.

[2] post-selected on unambiguous qubit preparation by Alice and detection by Bob.

Assumptions of Standard QKD

1. Quantum physics is the correct description of the world.
2. No information (quantum or classical) can leave Alice's or Bob's lab which is not under their control.
3. Alice and Bob have secure random number generators.
4. Alice's preparation device, and Bob's detector are *trustworthy*.

Note that no limitation is put on Eve's ability. She may use a *coherent attack*: intercept all n of the qubits Alice sends, process them using a huge quantum computer, and send them on to Bob.

Alice's preparation can be replaced by an *untrusted, external source of entanglement*. In this case the last assumption is weakened to

4. Alice's and Bob's detectors are *trustworthy*,

and the key rate becomes $r = \eta_B \eta_A [1 - h(Q_X^{\rm ps}) - h(Q_Z^{\rm ps})]$

Assumptions of Standard QKD

1. Quantum physics is the correct description of the world.
2. No information (quantum or classical) can leave Alice's or Bob's lab which is not under their control.
3. Alice and Bob have secure random number generators.
4. Alice's preparation device, and Bob's detector are *trustworthy*.

Note that no limitation is put on Eve's ability. She may use a *coherent attack*: intercept all n of the qubits Alice sends, process them using a huge quantum computer, and send them on to Bob.

Alice's preparation can be replaced by an *untrusted, external source of entanglement*. In this case the last assumption is weakened to

4. Alice's and Bob's detectors are *trustworthy*,

and the key rate becomes $r = \eta_B \eta_A [1 - h(Q_X^{\rm ps}) - h(Q_Z^{\rm ps})]$

Assumptions of Standard QKD

1. Quantum physics is the correct description of the world.
2. No information (quantum or classical) can leave Alice's or Bob's lab which is not under their control.
3. Alice and Bob have secure random number generators.
4. Alice's preparation device, and Bob's detector are *trustworthy*.

Note that no limitation is put on Eve's ability. She may use a *coherent attack*: intercept all n of the qubits Alice sends, process them using a huge quantum computer, and send them on to Bob.

Alice's preparation can be replaced by an *untrusted, external source of entanglement*. In this case the last assumption is weakened to

4. Alice's and Bob's detectors are *trustworthy*,

and the key rate becomes $r = \eta_B \eta_A [1 - h(Q_X^{\rm ps}) - h(Q_Z^{\rm ps})]$

Device-Independent QKD

1. Quantum physics is the correct description of the world.
2. No information (quantum or classical) can leave Alice's or Bob's lab which is not under their control.
3. Alice and Bob have secure random number generators.[3]
4. ~~Alice's and Bob's detectors are *trustworthy*.~~

This protocol [Acín *et al.*, PRL (2007).] again uses an (untrusted, external) entangled source, and the best key rate[4] is

$$r = \eta_A \eta_B [1 - h(Q_Z^{\rm ps})] - \log_2 \left[1 + \sqrt{2 - (S/2)^2}\right],$$

where S is the *non-post-selected* CHSH parameter. i.e. Bell nonlocality ($S > 2$) is necessary, but not sufficient, for a secure key.

[3] But one does need the technical assumption that the detectors are memoryless.

[4] Branciard, ... , Wiseman, Phys. Rev. A (Rapid Comm.) **85**, 010301(R) (2012).

Device-Independent QKD

1. Quantum physics is the correct description of the world.
2. No information (quantum or classical) can leave Alice's or Bob's lab which is not under their control.
3. Alice and Bob have secure random number generators.[3]
4. ~~Alice's and Bob's detectors are *trustworthy*.~~

This protocol [Acín *et al.*, PRL (2007).] again uses an (untrusted, external) entangled source, and the best key rate[4] is

$$r = \eta_A \eta_B [1 - h(Q_Z^{\rm ps})] - \log_2 \left[1 + \sqrt{2 - (S/2)^2}\right],$$

where S is the *non-post-selected* CHSH parameter. i.e. Bell nonlocality ($S > 2$) is necessary, but not sufficient, for a secure key.

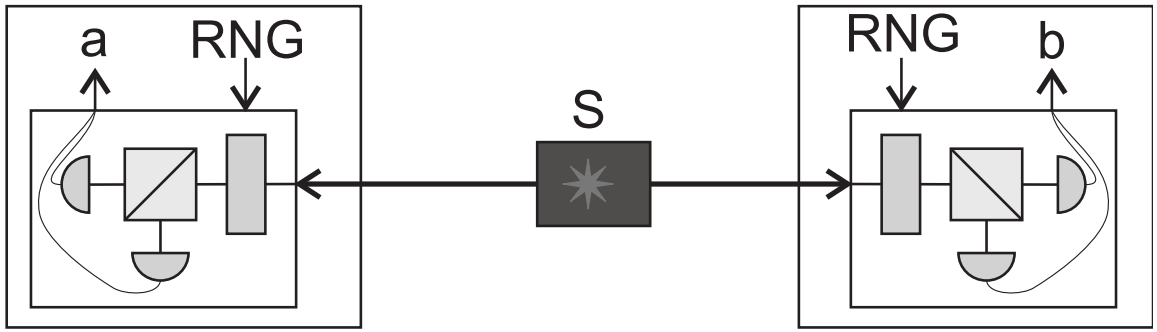
[3] But one does need the technical assumption that the detectors are memoryless.

[4] Branciard, ... , Wiseman, Phys. Rev. A (Rapid Comm.) **85**, 010301(R) (2012).

Three types of Entanglement-based QKD

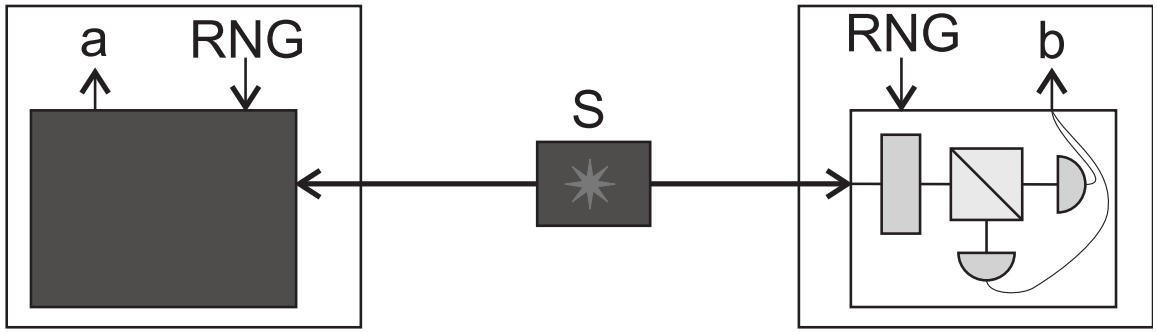
(i) S-QKD

Entanglement



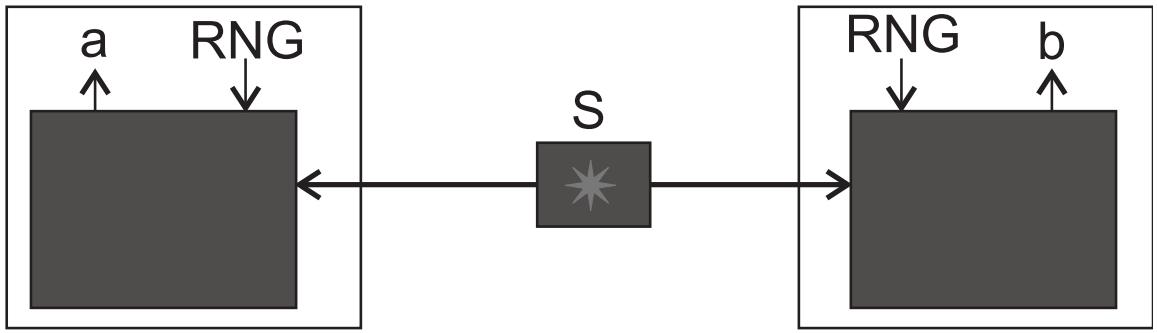
(ii) 1sDI-QKD

EPR-steering



(iii) DI-QKD

Bell nonlocality



1-sided Device-Independent QKD

1. Quantum physics is the correct description of the world.
2. No information (quantum or classical) can leave Alice's or Bob's lab which is not under their control.
3. Alice and Bob have secure random number generators.
4. **Bob**'s detector is *trustworthy*. [5]

Our protocol [Branciard, Cavalcanti, Wallborn, Scarani & Wiseman, Phys. Rev. A (Rapid Comm.) **85**, 010301(R) (2012)] has a key rate

$$r = \eta_B\{\eta_A[1 - h(Q_Z^{\mathrm{ps}})] - h(Q_X^{\mathrm{ps(B)}})\}.$$

Note that EPR-steering requires only the standard (X and Z) QKD measurements, and it can be shown that EPR-steering is necessary, but not sufficient, for a secure key.

[5] Again for *coherent attacks* we must assume Alice's detector is memoryless.

1-sided Device-Independent QKD

1. Quantum physics is the correct description of the world.
2. No information (quantum or classical) can leave Alice's or Bob's lab which is not under their control.
3. Alice and Bob have secure random number generators.
4. **Bob**'s detector is *trustworthy*. [5]

Our protocol [Branciard, Cavalcanti, Wallborn, Scarani & Wiseman, Phys. Rev. A (Rapid Comm.) **85**, 010301(R) (2012)] has a key rate

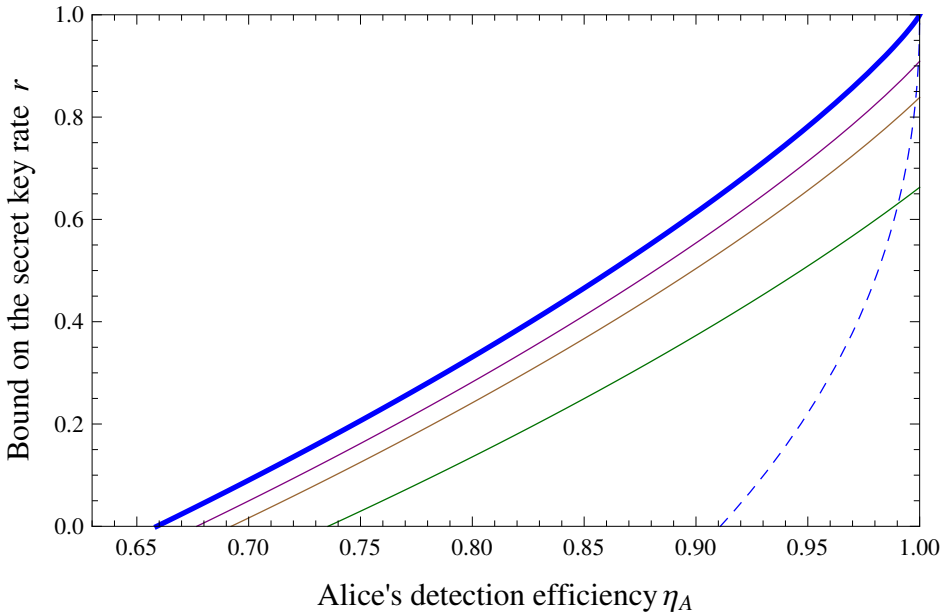
$$r = \eta_B\{\eta_A[1 - h(Q_Z^{\mathrm{ps}})] - h(Q_X^{\mathrm{ps(B)}})\}.$$

Note that EPR-steering requires only the standard (X and Z) QKD measurements, and it can be shown that EPR-steering is necessary, but not sufficient, for a secure key.

[5] Again for *coherent attacks* we must assume Alice's detector is memoryless.

Comparison of Key Rates and Thresholds

Type	AD	C	S	C	BD	Efficiency Thresholds
P&M	T	T	T	U	T	none
P&M	U	T	T	U	T	$[\mu_A > 65.9\%]$
P&M	U	U	T	T	T	$\eta_A > 65.9\%$
P&M	U	U	T	T	U	$\mu_B = 100\% \implies \eta_A > 83.3\%$
Entang.	T	U	U	U	T	none
EPR-S	U	U	U	U	T	$\eta_A > 65.9\%$
Bell	U	U	U	U	U	$\eta_A = \eta_B = \eta \implies \eta > 91.1\%$



Dotted: Best rate for DI-QKD, perfect visibility.

Solid: Best rates for 1sDI-QKD, visiblity = 1, 0.99, 0.98, 0.95.

Note $r \propto \eta_B$, here set $= 100\%$.

Related Papers and Future Possibilities

nature COMMUNICATIONS

OPEN

ARTICLE

Received 3 Aug 2011 | Accepted 30 Nov 2011 | Published 10 Jan 2012

DOI: 10.1038/ncomms1628

Conclusive quantum steering with superconducting transition-edge sensors

Devin H. Smith[1,2], Geoff Gillett[1,2], Marcelo P. de Almeida[1,2], Cyril Branciard[2], Alessandro Fedrizzi[1,2], Till J. Weinhold[1,2], Adriana Lita[3], Brice Calkins[3], Thomas Gerrits[3], Howard M. Wiseman[4], Sae Woo Nam[3] & Andrew G. White[1,2]

PHYSICAL REVIEW X **2**, 031003 (2012)

Arbitrarily Loss-Tolerant Einstein-Podolsky-Rosen Steering Allowing a Demonstration over 1 km of Optical Fiber with No Detection Loophole

A. J. Bennet,[1,2] D. A. Evans,[1,2] D. J. Saunders,[1,2] C. Branciard,[3] E. G. Cavalcanti,[2,4] H. M. Wiseman,[1,2,*] and G. J. Pryde[1,2,†]

Outline

Summary, and Other Work

- EPR-steering:
  - Only formulated rigorously in 2007.
  - First loop-hole-free experiment in 2012.
- Subjectivity (detector-dependence) of quantum jumps
  - An attribute of quantum jump theory never rigorously tested.
  - We have proposed a **realistic** experiment to prove the subjectivity of quantum jumps on a resonantly driven 2LA.
  - This generalizes EPR-steering to a continuously monitored system.
- 1-sided Device-Independent Quantum Key Distribution
  - We have developed this new asymmetric protocol.
  - More secure than standard QKD, more feasible than DI-QKD.
  - Inspired by, and requires, EPR-steering.
- New work: Showing that Buscemi's [PRL, 2012] "semi-quantum games" are actually *quantum-refereed entanglement witnesses*, and generalizing them to *quantum-refereed steering tests*. [Cavalcanti, Hall, & Wiseman, arxiv:1210.6051].