Detecting faked continuous-variable entanglement using one-sided device-independent entanglement witnesses

B. Opanchuk, L. Arnaud, and M. D. Reid*
Centre for Quantum and Optical Science, Swinburne University of Technology, Melbourne, Victoria 3122, Australia
(Received 23 December 2013; published 3 June 2014)

We demonstrate the principle of one-sided device-independent continuous-variable (CV) quantum information. In situations of no trust, we show by enactment how the use of standard CV entanglement criteria can mislead Charlie into thinking that Alice and Bob share entanglement, when the data are actually generated classically using a local-hidden-variable theory based on the Wigner function. We distinguish between criteria that demonstrate CV entanglement, and criteria that demonstrate the CV Einstein-Podolsky-Rosen (EPR) steering paradox. We show that the latter, but not the former, are necessarily one-sided device-independent entanglement witnesses, and can be used by Charlie to signify genuine EPR entanglement, if he trusts only Alice. A monogamy result for the EPR steering paradox confirms the security of the shared amplitude values in that case.

DOI: 10.1103/PhysRevA.89.062101 PACS number(s): 03.65.Ud, 03.67.Dd, 03.67.Hk, 03.67.Mn

I. INTRODUCTION

The importance of *trust*, either of an observer or of the devices employed, has motivated the emergence of "a new paradigm" [1] in the field of quantum information: device-independent (DVI) quantum information processing [1–7]. In light of this emergence, it is now recognized that quantum nonlocality has a very special role to play in quantum information. In a classic scenario, Charlie wants to confirm whether the qubit values reported to him by Alice and Bob have been generated from an entangled quantum source. For quantum key distribution (QKD), this may allow him to deduce that these values are not known to any eavesdropper Eve [8,9]. Quite surprisingly, if Charlie uses certain entanglement criteria, called device-independent entanglement witnesses (DVIEWs), he does not have to assume anything about the exact nature of the devices Alice and Bob are using or the reliability of their measurements [2,3,10,11].

Device-independent entanglement witnesses are those introduced by Bell, that demonstrate not only quantum entanglement, but quantum nonlocality [2–4]. If Charlie verifies violation of a Bell inequality, he can be sure the statistics did not arise from any local-hidden-variable (LHV) theory [12]. The concept of quantum nonlocality is distinct from that of entanglement, and DVI security is not given by all entangled states. A problem for the implementation of DVI quantum information however is that when most photons are not detected, not all LHV theories can be eliminated [13–17]. These sorts of "loophole" issues are often overcome by continuous-variable (CV) quantum information. Here, information is carried in the amplitudes of fields, enabling efficient detection and transmission [18–24]. A second problem then arises. The most widely used CV entangled resource (the two-mode squeezed state) has an LHV description, for the results of Alice and Bob's amplitude measurements [25,26,28]. This means that those amplitude values will not violate a Bell inequality.

The amplitude values of the CV entangled resource do display quantum nonlocality however: namely, the nonlocality presented by Einstein, Podolsky, and Rosen (EPR) [27] in their 1935 EPR paradox [29]. EPR's nonlocality addresses whether the action of measurement by Bob can immediately influence the results of Alice's *quantum* measurements at another distant site. EPR demonstrate their paradox, by assuming that values at Alice's location arise from measurements of quantum observables. There is no similar assumption for Bob's measurements. The EPR paradox is realized through a procedure that is "one-sided device-independent," and criteria for the EPR paradox, unlike those for "EPR entanglement," are "one-sided" DVIEWs.

The concept of *one-sided device-independent* security has been pioneered in Refs. [30–32], based on the resource of quantum steering [33]. In fact, the EPR paradox is an example of quantum steering [31,32,34]. The analysis [30] focused on QKD with qubits, but revealed advantages, if one is justified in assuming trust at *one* site. The advantages are implicit in previous work on CV QKD based on criteria that relate to the EPR paradox [19,20,35]. Clearly, this concept has the potential to introduce the new DVI paradigm to CV quantum information.

Here, we demonstrate the principle and feasibility of CV one-sided DVI quantum information. We do this in three steps:

(1) First, we illustrate the vulnerability of CV quantum information in situations of no trust, if one uses standard entanglement criteria such as that derived by Duan *et al.* [36] and Simon [37]. Our illustration is by enactment: where neither Alice and Bob can be trusted, we deceive Charlie by simulating entanglement trivially using a classical computer. We next show that even if Alice can be trusted, we can still deceive Charlie if he uses a criterion that is not a one-sided DVIEW. The "faked" entanglement can be generated using an unsophisticated hybrid scheme involving classical computers and a classical optical source. We also discuss the motivation by a malicious Eve to fake the entanglement—so that she can fool Charlie into thinking a set of amplitude values are held securely between the two parties Alice and Bob, when in fact they can be distributed by her to an infinite number of parties.

(2) Second, we prove that if Charlie confirms a one-sided DVI EPR paradox criterion *and* he trusts Alice, he can be sure the results do originate from an EPR entangled state.

(3) Lastly, we use a monogamy result [35,38,39] for the EPR paradox to show that confirmation of the EPR paradox

*mdreid@swin.edu.au

criterion is enough to give security against an eavesdropper Eve possessing a noise-free replica of the amplitude values, despite the fact that Bob cannot be trusted.

Practical implementation of CV one-sided DV security requires demonstration of an EPR steering paradox, which is more generally difficult than entanglement [40]. Nonetheless, the CV EPR paradox has been verified without fair sampling loopholes for a range of optical systems [25,26,41]. These will be briefly discussed in the Conclusion. The elimination of the "locality" loophole is also important [17], if CV DVI is to become a reality. Since security is often comprised at one site only, we expect CV one-sided DVI protocols to become useful.

II. DETECTING SHARED ENTANGLEMENT

Let Alice and Bob be two spatially separated observers at stations labeled A and B respectively. Suppose an observer at a central station sends to Alice one of the quantum subsystems that comprise a CV EPR state, and to Bob the other. A sequence of similarly prepared states is transmitted. After each transmission t_i, an observer Charlie selects randomly to ask Alice and Bob to measure either the position X or the momentum P of the subsystems at their respective stations (or sites), and to report to him the values of their measurements [8,9,19–22]. A CV EPR state is a simultaneous eigenstate of momentum sum and position difference, and the values given by Alice and Bob will be accordingly correlated. If Charlie determines that these values satisfy an entanglement criterion, then he can confirm that Alice and Bob indeed share an entangled state.

A. Duan-Simon criteria for CV entanglement

The most widely used CV EPR entanglement criterion is based on the methods of Duan *et al.* and Simon [36,37,42]. Entanglement between the systems measured by Alice and Bob is confirmed if

$$\mathrm{Ent} = \frac{4}{(1+g^2)}\Delta(X_A - gX_B)\Delta(P_A + gP_B) < 1, \qquad (1)$$

where g is any real constant and we use the notation $(\Delta X)^2 \equiv \langle X^2\rangle - \langle X\rangle^2$. Here, $X_{A/B}$ and $P_{A/B}$ are the "position" and "momentum" quadratures measured by Alice and Bob respectively, and we have selected a suitable scaling so that the Heisenberg quantum uncertainty principle is written $\Delta X\Delta P \geqslant 1/4$. Clearly, the CV EPR state will satisfy the condition (1), with $g = 1$. For more general states, the choice of g is taken optimally so that the left side of the inequality (1) is minimized. For the Gaussian systems that are most commonly utilized for CV quantum information processing (QIP) [18], and restricting attention to a subclass of Gaussian states with symmetry between position and momentum correlation, this criterion can be shown to be *necessary and sufficient* for detecting bipartite entanglement [36,38,43]. Generally speaking, however, an entanglement criterion cannot detect entanglement for all systems, and is hence only *sufficient* to detect (witness) entanglement. Therefore, throughout this paper, we will use the terms "criterion" and "witness" interchangeably, to mean the same thing.

Before continuing, it is important to understand the assumptions needed in deriving the criterion (1) (and other very similar criteria), since it is these assumptions that create the security loopholes addressed by device-independent quantum information processing. To derive the criterion (1), one begins by supposing that the bipartite system of Alice and Bob is nonentangled. By definition of entanglement, this means that the bipartite density operator can be written in the separable form [44]

$$\rho_{AB} = \sum_R P(R)\rho_A^R\rho_B^R \qquad (2)$$

where here $\sum_R P(R) = 1$ and ρ_A^R and ρ_B^R are quantum density operators for Alice's system A and Bob's system B alone. The uncertainty product for the separable mixture is constrained by the uncertainty product for the product states that are the components of the mixture. For product states $\rho_A^R\rho_B^R$ we can write

$$\begin{aligned}&\Delta_R(X_A - gX_B)\Delta_R(P_A + gP_B)\\ &\quad\geqslant \Delta_R X_A\Delta_R P_A + g^2\Delta_R X_B\Delta_R P_B\end{aligned} \qquad (3)$$

where we write the subscript R to remind us that the averages are with respect to the component state R (see Refs. [36,37,42] for full details). Using the fact that ρ_A^R and ρ_B^R are *quantum* states, the Heisenberg uncertainty relation applies to each, and it follows that

$$\Delta_R(X_A - gX_B)\Delta_R(P_A + gP_B) \geqslant \tfrac{1}{4}(1+g^2). \qquad (4)$$

Thus, if (1) is satisfied, the two systems A and B cannot be represented by (2) and must therefore be entangled.

The crucial assumption for the practical application of the criterion by Charlie is that both sets of values X_A, P_A and X_B, P_B, are truly outcomes of measurements of the quantum observables, and are hence correctly constrained for all possible local component states ρ_A^R, ρ_B^R by the Heisenberg uncertainty relations: $\Delta_R X_A\Delta_R P_A \geqslant 1/4$ and $\Delta_R X_B\Delta_R P_B \geqslant 1/4$. If Alice and Bob do not report the results of quantum measurements, the criterion cannot be applied to faithfully detect entanglement [4,30,31]. *Both Alice and Bob must be trusted.*

We remark that the well-known simple "Duan" criterion [36] detects entanglement between A and B if

$$[\Delta(X_A - X_B)]^2 + [\Delta(P_A + P_B)]^2 < 1. \qquad (5)$$

This criterion follows directly from the criterion (1), by taking $g = 1$ and noting that for any real numbers x and y, $x^2 + y^2 \geqslant 2xy$. Hence, if the simple criterion detects entanglement, so will the more powerful criterion (1) [42], provided g is optimally chosen. Thus, the results of this paper are applicable if criterion (5) is used instead of (1).

B. EPR steering criterion as a one-sided DVI criterion for entanglement

Entanglement can also be confirmed by the EPR paradox [26,27]. Such a paradox (also called an EPR steering paradox [31,32,34]) is realized if [29]

$$\mathrm{EPR}_{A|B} = 4\Delta_{\mathrm{inf}}X_{A|B}\Delta_{\mathrm{inf}}P_{A|B} < 1, \qquad (6)$$

where $(\Delta_{\rm inf} X_{A|B})^2$ is the average variance of the conditional distribution for the measurement X_A given a measurement at B [26,29,35], and $(\Delta_{\rm inf} P_A)^2$ is defined similarly. The subscript "inf" reminds us of the original formulation of the EPR paradox, in which the emphasis is on an observer, here called Bob, who can make a near-perfect inference of the outcome of a measurement by Alice, even though he is spatially separated from Alice's measurement station. For Gaussian systems, meaning Gaussian states and measurements, this criterion has been shown necessary and sufficient to detect EPR steering [32].

On selecting $(\Delta_{\rm inf} X_A)^2$ and $(\Delta_{\rm inf} P_A)^2$ to be the variances conditional on measurements X_B, and P_A, respectively, we see that the CV EPR state will satisfy this EPR condition. The EPR paradox criterion can then more specifically be written as [26,29]

$$\mathrm{EPR}_{\mathrm{A|B}} = 4\Delta(X_A - gX_B)\Delta(P_A + gP_B) < 1, \qquad (7)$$

where g is a real constant optimized so that the left side of inequality (7) is minimized.

We now briefly summarize the assumptions needed to derive the EPR criteria, for comparison with those needed to derive the Duan-Simon-type entanglement criteria. The key point is that the EPR steering criteria are based on fewer assumptions, and are useful for CV one-sided DVI [30] quantum information processing.

The EPR criteria can be derived using the extension of EPR's argument, in which Bob is able to predict the result for Alice's X_A or P_A measurement to an uncertainty given by $\Delta_{\rm inf} X_A$ and $\Delta_{\rm inf} P_A$, respectively [26,29]. In their argument, EPR make the assumption that certain premises [referred to as EPR's local realism (LR)] will hold. They use these premises to deduce that there is a local realistic description for Alice's measurements, in which the results for X_A and P_A are *simultaneously* predetermined to a precision $\Delta_{\rm inf} X_A$ and $\Delta_{\rm inf} P_A$, which of course when $\Delta_{\rm inf} X_A \Delta_{\rm inf} P_A < 1/4$ contradicts any local quantum state description. Then the EPR paradox is established, because LR implies a local description at A that is inconsistent with (the completeness of) quantum mechanics.

The alternative approach in which the EPR paradox criterion (6) [or (7)] is proven to be one for EPR steering involves similar assumptions [34]. In fact, the proofs for EPR steering follow along parallel lines to those for entanglement. For the EPR steering proof, separability takes the more general form of Bell's local-hidden-variable model [12]. This may be likened to the first step in the EPR argument, where the assumption of EPR's local realism is made [35]. On expansion, we see that the criteria involve second-order moments such as $\langle X_A^\theta X_B^\phi \rangle$ where $X_{A/B}^\theta = X_{A/B}\cos\theta + P_{A/B}\sin\theta$ ($\theta = 0$ or $\pi/2$). For all LHV models, these can be expressed in the separable form

$$\langle X_A^\theta X_B^\phi \rangle = \int P(\lambda) \langle X_A^\theta \rangle_\lambda \langle X_B^\phi \rangle_\lambda d\lambda, \qquad (8)$$

where λ are classical hidden-variable parameters and $P(\lambda)$ is the probability distribution for these parameters. The λ correspond to the R in (2) and at the various steps in the proof. $\langle X_A^\theta \rangle_\lambda$ is the average value for the result X_A^θ, given the hidden-variable state specified by λ. $\langle X_B^\phi \rangle_\lambda$ is defined similarly. Manipulation based on this LHV assumption reveals that the result (3) will once more hold, but with λ replacing R. However, after this step, unlike the proof for entanglement, the two subsystems are treated asymmetrically. For Alice's measurements, consistency with local quantum states ρ_A^λ is again assumed, so that the Heisenberg uncertainty relation holds, i.e., $\Delta_\lambda X_A \Delta_\lambda P_A \geqslant \frac{1}{4}$. This may be likened to the step in the EPR argument where the "elements of reality" for Alice's local states are compared for consistency with quantum mechanics [35]. However, no such assumption is made about Bob's local system or measurements. It is assumed only that the variances are positive, i.e., $\Delta_\lambda X_B \Delta_\lambda P_B \geqslant 0$. With these assumptions, we find

$$\Delta_\lambda(X_A - gX_B)\Delta_\lambda(P_A + gP_B) \geqslant \tfrac{1}{4}. \qquad (9)$$

The LHV model with the additional constraint for local states at A is called a local-hidden-state (LHS) model [31]. This LHS model will imply $\Delta(X_A - gX_B)\Delta(P_A + gP_B) \geqslant \frac{1}{4}$. The inequality (7) [as for (6)] therefore implies an EPR paradox and EPR steering of A by B [31,34].

We see from both derivations that it is necessary to assume Alice does indeed report the results of the appropriate quantum measurements, if the EPR steering criterion [(6) or (7)] is to be valid. However, unlike the Duan-Simon entanglement criteria, it is not necessary to make this assumption about Bob's measurements. Thus, the criterion is independent of the devices used at Bob's measurement station. Regardless of the orgin of Bob's values, the criterion is still valid for detecting the EPR steering paradox. *Only Alice must be trusted.*

In detecting the EPR steering paradox, the EPR criterion will also detect entanglement [26,31]. This is because any separable description (2) will also imply the LHV expansion (8), with or without the assumption of the uncertainty relation $\Delta_\lambda X_A \Delta_\lambda P_A \geqslant \frac{1}{4}$, and therefore cannot generate an EPR steering paradox. Separable models are subsets of LHV and LHS models. The EPR criterion is therefore a *one-sided device-independent criterion* for entanglement.

It has been observed [40,43] that the EPR paradox criterion (6) is less robust to noise and losses than the Duan-Simon entanglement criterion (1). The EPR paradox criterion does not detect all entangled states. This is because of the different assumptions made about the nature of Bob's measurements. For Eq. (1), the measurements X_B and P_B at Bob's location must genuinely correspond to those of the quantum conjugate observables. For the EPR criterion, this assumption about Bob's measurements is not made. The EPR criterion (6) makes fewer assumptions than can be justified if one can indeed trust Alice and Bob to make the right measurements, and is as a consequence a less sensitive witness of entanglement. The criterion is generally more difficult to satisfy, but has the advantage of being (equivalent to) a one-sided DVIEW [2–4].

III. FAKING CV ENTANGLEMENT

It may be that Alice and Bob (or their devices) *cannot* be trusted, and do not report to Charlie the values of measured quantum quadrature phase amplitudes. Instead, they may report values that have been created by a classical computer simulation. Then, we will show that the entanglement criteria of the last section can be satisfied even though there is no

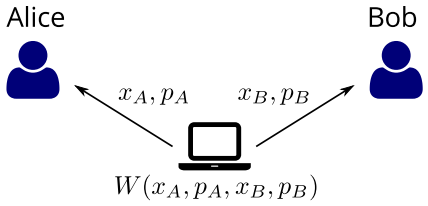

FIG. 1. (Color online) Faking the CV entanglement using classical protocols where the measurement stations of Alice and Bob cannot be trusted. A sequence of two classical-number pairs representing position and momentum are generated probabilistically (by Eve) from the computer using the Wigner function (11). These are sent to Alice and Bob, where they are stored locally. Alice and Bob fake entanglement by reporting these numbers to Charlie, who then verifies "entanglement" using either the Duan-Simon criterion (1) or the EPR criterion (6) [Fig. 3, curves (a) and (b)]. Security is compromised because the amplitude values can be shared by an infinite number of parties in this case.

entanglement. We call this "faked entanglement." The faking of the entanglement is possible, because the assumptions made in the derivation of the criteria are no longer valid. In this paper, we illustrate the faking of entanglement in two scenarios: first, where neither Alice nor Bob can be trusted (Fig. 1), in which case neither criterion (1) nor (6) is valid; and second, where only Alice can be trusted (Fig. 2), in which case only the EPR criterion (6) is valid.

The implications can be understood by considering a motivation for the faking protocol. In the scenario of Sec. II, Charlie has transmitted to Alice and Bob the particles or light fields

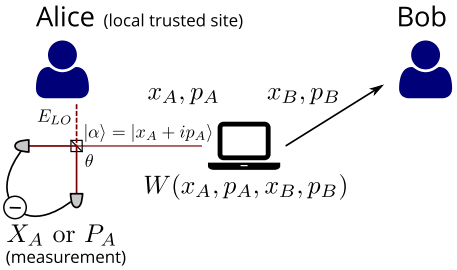

FIG. 2. (Color online) Faking the CV entanglement in the case where Alice can be trusted: The scenario is similar to Fig. 1 but now Alice can be trusted to report to Charlie the results of measurements of genuine quantum observables $\hat{X}_A$ and $\hat{P}_A$. Bob, however, cannot be trusted. Entanglement satisfying the Duan-Simon criterion (1) can still be faked using the asymmetric hybrid protocol depicted, involving the computer and a coherent-state light source $|\alpha\rangle$ (where $\alpha = x_A + ip_A$) that is deviously input to Alice's site [Fig. 3, curve (c)]. The entanglement detected by the EPR criterion (6), however, cannot be faked by one-sided scenarios where Alice is trusted [Fig. 3, curve (d)]. If violated in the one-sided scenario, the EPR criterion detects genuine entanglement, and [through the monogamy result (20)] gives quantifiable security against all processes that would allow distribution of the amplitude values. In the picture, Alice measures the quadrature amplitudes $\hat{X}_A$ and $\hat{P}_A$ of the field at her location using a standard homodyne measurement scheme, where the field is combined across a beam splitter with an intense local oscillator field (denoted $E_{\rm LO}$). The variable phase shift θ allows her to choose whether $\hat{X}_A$ or $\hat{P}_A$ is measured.

that form the two subsystems of an entangled EPR state. He wants Alice and Bob to report the results of their measurements of either X or P at each site, for a sequence t_i of such transmissions, so that he can confirm entanglement by taking the appropriate averages required by the entanglement criterion (1) or (6). Once he confirms entanglement, the amplitude values that are shared by Alice and Bob become useful for QIP tasks, for example, for CV quantum key distribution [8,21]. The sequence t_i that is used to test for entanglement does not have to be exhaustive, so a sequence of unrevealed correlated amplitudes can remain secret to the stations of Alice and Bob. Now suppose a devious Eve seeks to trick Charlie, Alice, and Bob. We will show how she can create from a computer a sequence of numbers x_A, p_A, x_B, p_B that mimic the results for measurements X_A, P_A, X_B, P_B, respectively, in that they will satisfy the inequalities of the entanglement criteria (1) and (6). We call these "Eve's numbers." Each pair x_A, p_A of the sequence can be stored, in order, at Alice's station, and each associated pair x_B, p_B can be stored, in order, at Bob's station. Alice and Bob may be accomplices of Eve, or else it may be they are loyal to Charlie, but that their devices (e.g., a final readout computer) are tampered with by an infiltrator. Either way, if Charlie trusts the results that Alice and Bob report and believes they hold a sequence of values for amplitudes based on an entangled state, there could be serious consequences. The amplitudes of the whole sequence are *not* secure, but can be shared by an infinite number of parties, since the sequence is formerly known to Eve and can be distributed by her. The validity of QKD based on the assumption of an entangled state is destroyed.

We now illustrate by example the method of faking entanglement. The standard realization of the CV EPR state is the two-mode squeezed state [45]:

$$|\psi\rangle = \mathrm{sech}(r) \sum_{n=0}^{\infty} \tanh^n(r) |n\rangle_A |n\rangle_B \tag{10}$$

where $|n\rangle_{A/B}$ are the number states of modes at the locations A and B of Alice and Bob, respectively, and $r \geqslant 0$ is the squeeze parameter that determines the amount of entanglement between the modes of Alice and Bob. The Wigner function for this state is

$$W(\underline{x}) = \frac{4}{\pi^2} \exp\{-[(x_A - x_B)^2 + (p_A + p_B)^2]/\sigma_-^2 - [(x_A + x_B)^2 + (p_A - p_B)^2]/\sigma_+^2\}, \tag{11}$$

where $\sigma_+^2 = \exp(2r)$ and $\sigma_-^2 = \exp(-2r)$ and we introduce the notation $\underline{x} = (x_A, p_A, x_B, p_B)$ [46]. The moments of the quadrature phase amplitudes are given directly by the amplitude moments of the distribution. The positivity of the Wigner function allows for a perfectly accurate probabilistic simulation of the entangled *quadrature* correlations, based on the measurements of $X_{A/B}^{\theta}$. This fact, pointed out by Bell [47], is well known [25]. The implication is that if Charlie restricts himself to a criterion based on quadrature measurements, and if Alice and Bob or their devices cannot be trusted, he can be fooled into thinking there is entanglement shared between them when there is not.

Hence, a classical process that mimics the entangled correlations given by (1) and (6) is as follows. At transmission time t_i, a central source Eve generates with probability $W(\underline{x})$

the values x_A, p_A, x_B, and p_B, and sends them to Alice and Bob (Fig. 1). The process is repeated N times, a different set of numbers being probabilistically generated on each trial t_i. When Charlie calls for the value of transmission t_i, Alice gives to him the value x_A or p_A, depending on whether Charlie asked her (and Bob) to measure position or momentum. Similarly, Bob reports his value, x_B or p_B. Charlie evaluates the averages as required for the criteria (1) and (6). The averages are precisely consistent with the predictions of the two-mode squeezed state, and both criteria are satisfied for all r. Specifically, we find [on selecting the optimal value for g in (1), namely $g = 1$]

$$\mathrm{Ent} = \exp(-2r) \tag{12}$$

and [on optimizing the choice of measurements at B and selecting the optimal value for g in (7), namely, $g = \tanh 2r$ [29]]

$$\mathrm{EPR}_{A|B} = \mathrm{sech}(2r). \tag{13}$$

We have carried out the procedure of Fig. 1, and illustrate the faking of the quantum entanglement by classical means in Figs. 3–5. A possible set of Eve's numbers is presented in Fig. 5. Despite the fact that the data satisfy the entanglement criteria (1),(5) and (6),(7), there is no possibility of security,

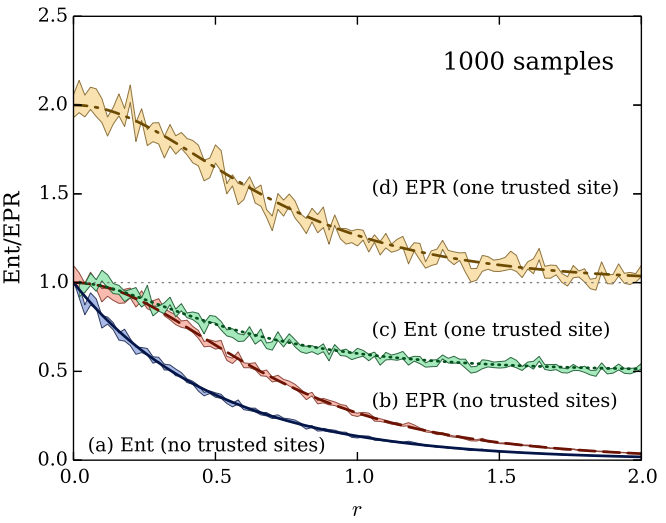

FIG. 3. (Color online) Distinguishing faked from genuine entanglement using a one-sided device-independent entanglement criterion: Curves (a) and (b) plot the results for Ent and $\mathrm{EPR}_{A|B}$ as realized by the enactment of the classical protocol of Fig. 1, where neither Alice nor Bob can be trusted. Here, r is the squeeze parameter used in the Wigner function and there are $N = 1000$ trials. The bandwidths correspond to the sampling errors, centered on the sampled means. Both the entanglement certified by the Duan-Simon criterion and that certified by the EPR steering criterion are faked. Charlie can be fooled into thinking there is entanglement, if he mistakenly trusts Alice and Bob. Curves (c) and (d) plot the results for the enactment of the classical hybrid protocol of Fig. 2, where Alice can be trusted. The Duan-Simon entanglement criterion (1) can be faked [curve (c)], but *not* the EPR steering inequality (6) [curve (d)], which is a one-sided device-independent entanglement criterion. If Charlie trusts Alice, he can use the EPR criterion to distinguish faked from genuine entanglement.

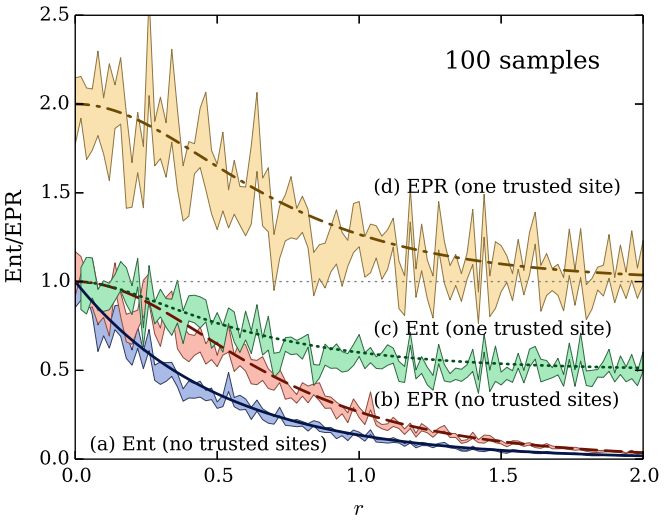

FIG. 4. (Color online) Distinguishing faked from genuine entanglement using a one-sided device-independent entanglement criterion: Curves as for Fig. 3, but where $N = 100$.

because the amplitude values can be distributed from the source (Eve) to an infinite number of other parties.

The undermining of the security occurs because neither of the entanglement criteria (1) or (6) used by Charlie are (equivalent to) DVIEWs. The particular moments evaluated

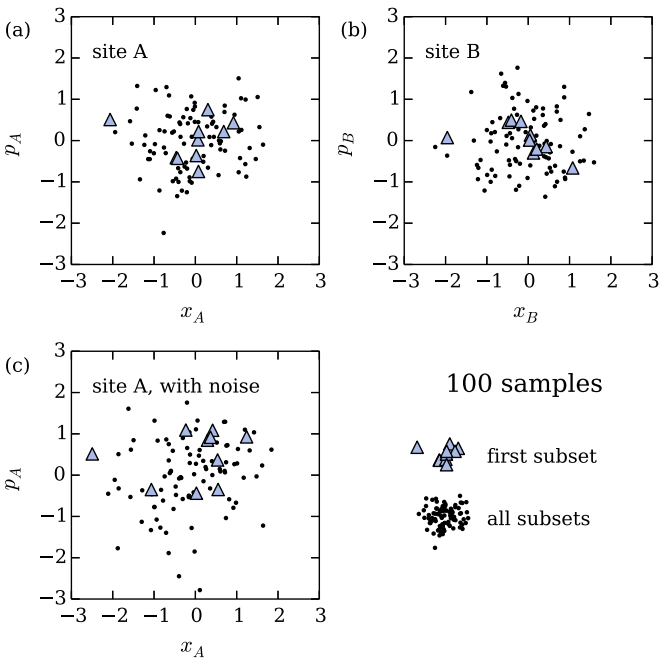

FIG. 5. (Color online) Actual values reported by Alice and Bob: (a) and (b) give a possible set of $\underline{x} = (x_A, p_A, x_B, p_B)$ for $N = 100$ trials where $r = 0.7$. Here, (a) gives the set of values for Alice, and (b) those for Bob. These are Eve's numbers, used for the purpose of faking entanglement (Fig. 1). (c) shows values for Alice, where the results are generated by the hybrid protocol of Fig. 2, in which case the values x_A and p_A correspond to the results of genuine quantum measurements $\hat{X}_A$ and $\hat{P}_A$. In this case, noise is added to the data. Triangles correspond to the first subset of ten samples used to calculate one of the samples for $\mathrm{EPR}_{A|B}$ or Ent.

by Charlie can be constructed using a local-hidden-variable (LHV) theory [2,3] based on the use of the positive Wigner function (11) [25,47]. This is true for all Gaussian states, defined as describable by a positive Gaussian Wigner function [18]. We give the explicit LHV construction for the moments as follows. As explained in the last section, the second-order moments needed for the criteria (1) and (6) are $\langle X_A^\theta X_B^\phi\rangle$ where $X_{A/B}^\theta = X_{A/B}\cos\theta + P_{A/B}\sin\theta$ ($\theta = 0$ or $\pi/2$). An LHV theory can generate these moments, if we can write

$$\langle X_A^\theta X_B^\phi\rangle = \int P(\lambda)\langle X_A^\theta\rangle_\lambda\langle X_B^\phi\rangle_\lambda d\lambda, \tag{14}$$

where λ are classical hidden-variable parameters and $P(\lambda)$ is the probability distribution for these parameters. $P(\lambda)$ is independent of the choice of measurement (θ and ϕ), which is made *after* the generation and separation of the subsystems. $\langle X_A^\theta\rangle_\lambda$ is the average value for the result X_A^θ, given the hidden-variable state specified by λ, and $\langle X_B^\phi\rangle_\lambda$ is defined similarly. For the classical simulation depicted in Figs. 1, 3, and 4, the Wigner variables $\underline{x}$ assume the role of Bell's hidden variables λ, $W(\underline{x})$ becomes $P(\lambda)$, and there is a deterministic situation whereby $\langle X_A^\theta\rangle_\lambda = x_A^\theta \equiv x_A\cos\theta + p_A\sin\theta$ and $\langle X_B^\phi\rangle_\lambda = x_B^\phi \equiv x_B\cos\phi + p_B\sin\phi$, so that $\langle X_A^\theta X_B^\phi\rangle = \langle x_A^\theta x_B^\phi\rangle$ [25,47].

A DVIEW would, like a Bell inequality, provide a criterion that if satisfied negates all LHV models. Thus, use of a device-independent entanglement criterion would allow Charlie to detect entanglement, by eliminating all of the LHV models, and therefore represents a more secure test of entanglement [4]. However, for the CV entanglement generated by the two-mode squeezed state, a DVIEW cannot be constructed directly from the amplitude X and P measurements only, since the LHV model (14) describes the statistics perfectly in this case [25,47]. We point out that, in view of the work of Banaszek and Wodkiewicz [48], this does not exclude DVI entanglement witnesses being constructed from other sorts of measurements. Also, the violation of a Bell inequality has been shown possible using quadrature phase amplitudes measurements, for more complex EPR-type sources [49].

IV. TWO TRUSTED MEASUREMENT STATIONS

It should be emphasised that Charlie can safely conclude genuine entanglement based on the criterion (1) or (6), if he can trust that the "measurement values" reported by Alice and Bob are genuinely the results of the quantum observables $\hat{X}_{A/B}$ and $\hat{P}_{A/B}$. Let us reexamine the derivation of the criteria, as outlined in Sec. II, to clarify this point.

Entanglement is defined as the failure of *quantum* separability. For any quantum-separable state [44], $\rho_{AB} = \sum_R P(R)\rho_A^R\rho_B^R$, which implies that the moments can be expressed as (on identifying R as a hidden variable λ)

$$\langle X_A^\theta X_B^\phi\rangle \equiv \langle \hat{X}_A^\theta \hat{X}_B^\phi\rangle = \int P(\lambda)\langle x_A^\theta\rangle_\lambda\langle x_B^\phi\rangle_\lambda d\lambda, \tag{15}$$

where $\langle x_A^\theta\rangle_\lambda$ and $\langle x_B^\phi\rangle_\lambda$ are additionally constrained to be the moments of *quantum* states ρ_A^λ and ρ_B^λ. Each predetermined local state (as specified by λ) is required to satisfy the quantum uncertainty relations. It is this fact which prevents a perfect correlation between Alice and Bob's "real" positions and momenta—unless there is entanglement. The criteria (1) and (6) falsify the quantum-separable model (15), but not the local-hidden-variable model (14) [31,32,34].

In the classical simulation based on (14), the predetermined local states are given by the classical numbers $\{x_A, p_A\}, \{x_B, p_B\}$, all of which are predetermined with perfect accuracy: That is, they are not constrained by the uncertainty relation. If Alice's and Bob's detectors have been tampered with or are unreliable, the values reported could arise from such a classical simulation in which case there can be an unlimited number of replica sets $\{x_B, p_B\}$ distributed.

V. ONE TRUSTED MEASUREMENT STATION

We now turn to the case where *one* measurement station, that of Alice, can be trusted. In this scenario, we will show that the use of the one-sided DVIEW criterion (6) enables reliable witnessing of entanglement: That is, faked entanglement is detected as "not entangled", and the criterion is satisfied only when there is genuine entanglement. We expect the one-sided entanglement witness to be useful to the field of QIP, since protocols are often asymmetric with one station being more secure than the other [30,31].

With Bob's station not being trusted, it is generally more difficult to verify entanglement, since one cannot assume the values he reports are necessarily those of genuine quantum measurements. The conditions on the quantum separable model (15) are relaxed: For this scenario, we consider moments given by a separable model

$$\langle X_A^\theta X_B^\phi\rangle \equiv \langle \hat{X}_A^\theta X_B\rangle = \int P(\lambda)\langle x_A^\theta\rangle_\lambda\langle p_B^\phi\rangle_\lambda d\lambda, \tag{16}$$

where *only* $\langle x_A^\theta\rangle_\lambda$ is constrained to be consistent with a quantum density operator ρ_A^λ [31]. Unlike for the model (15), there is no similar constraint on B. This hybrid separable model, which is a superset of all quantum separable models (15), is called a local-hidden-state (LHS) model. The falsification of this model indicates the nonlocality of quantum (or EPR) steering [31,32,34], and also entanglement.

It has been proved in Ref. [34] that the EPR inequality $\mathrm{EPR}_{A|B} \geqslant 1$ holds for all LHS models (16). We have outlined this proof in Sec. II. Hence, the EPR criterion (6) (which shows an EPR steering of Alice's system) negates all of the LHS models (16). In this way, entanglement is demonstrated, *without* the assumption of quantum measurements for the values reported at Bob's location. On the other hand, the LHS model (16) does *not* imply the entanglement criterion (1). In short, statistics generated by a LHS model (16) can satisfy the entanglement criterion (1), but cannot satisfy the EPR paradox criterion (6).

We give a demonstration (Fig. 2) of how Charlie can be misled into thinking there is entanglement, if he uses the wrong criterion for this scenario where only Alice can be trusted. Bob in collusion with Eve may set up the following protocol. Alice would be expecting (at each trial or time t_i of the sequence) an input to her station, corresponding to the subsystem of the entangled state sent by Charlie. This subsystem may take the form of an optical beam or pulse, the mode corresponding to A in the two-mode squeezed state (10). Her station is

secure, so Eve and Bob cannot tamper with it. Instead, they decide to tamper with the input. Input to Alice's station at each trial are the values x_A, p_A that stem from the central classical computer source, as before. However, these cannot be the final inputs, as Alice passes on to Charlie only the results of genuine quantum measurements $\hat{X}_A, \hat{P}_A$, made locally on a real experimental system. Bob then comes up with a hybrid protocol: Alice's experimental system is deviously coupled to the input classical values x_A, p_A, so that the measurements she reports are those of $\hat{X}_A, \hat{P}_A$ on the quantum coherent state $|\alpha\rangle$ where $\alpha = x_A + ip_A$. Thus, the optical beam or pulse that arrives at Alice's station is not the subsystem A of the entangled state (10), but the optical coherent state $|\alpha\rangle$. The statistics from this hybrid classical scenario are describable by a LHS model (16). Although the extra local quantum uncertainty provided by the coherent state means that Bob and Eve cannot predict exactly the values that Alice will report, the correlation with the values x_B, p_B (which they do know) is good enough that the inequality of the Duan-Simon criterion (1) is satisfied (although not maximally). This makes it possible to fake entanglement certified by the Duan-Simon criterion.

The results of carrying out Bob and Eve's protocol are given in Fig. 3. In our simulation, Alice does not actually measure the amplitudes of the optical coherent state. Instead, we model the outcomes of her measurement using standard quantum theory, by adding an appropriate noise source to the input classical numbers x_A, p_A. We note that the simulation results are in agreement with the predictions of a two-mode squeezed state (10) which is then coupled at Alice's location to a local quantum coherent-state noise source. The final mode which Alice measures is $X_{A'} = X_A + X_{\rm coh}$ where $\langle X_{\rm coh}, X_{\rm coh}\rangle = 1/4$. Calculation of the Duan-Simon–type criterion (1) gives

$$\mathrm{Ent} = \frac{4}{(1+g^2)}\{n - 2gc + g^2 m\}, \tag{17}$$

where $n = \langle X_{A'}, X_{A'}\rangle = \frac{1}{4}\{1 + \cosh(2r)\}$, $m = \langle X_B, X_B\rangle = \cosh(2r)/4$, and $c = \langle X_A X_B\rangle = \sinh(2r)/4$, and $\langle X, Y\rangle = \langle XY\rangle - \langle X\rangle\langle Y\rangle$. The entanglement measured by (1) is optimized for the choice $g = [n - m + \sqrt{(n-m)^2 + 4c^2}]/(2c)$. For Gaussian distributions, the minimum possible $[\Delta_{\rm inf}(X_A)]^2$ is given by the minimum value of $\langle[\Delta(X_{A'} - g_{\rm EPR} X_B)]^2\rangle = n + g_{\rm EPR}^2 m - 2g_{\rm EPR} c$ where $g_{\rm EPR}$ is a real constant [26,29]. Selecting $g_{\rm EPR} = c/m$, we find

$$\mathrm{EPR}_{A|B} = 1 + \mathrm{sech}(2r) \tag{18}$$

which, consistent with our knowledge of the LHS model (16), *cannot* satisfy the EPR steering criterion (6). Yet we see (Fig. 3) that the entanglement criterion (1) is satisfied for all values of r.

We remark that all of the EPR steering inequalities [34,50,51] that falsify the model (16) will suffice as a one-sided DVIEW [30]. One such criterion is [26,52]

$$\mathrm{Ent} < 0.5 \tag{19}$$

as evident in Fig. 3. However, for Gaussian states and measurements, the EPR criterion (6) has been shown necessary and sufficient to detect EPR steering, whereas the criterion (19) is not [31,32]. The EPR criterion is therefore a better witness, as can be important when asymmetry exists between the stations of Alice and Bob [53–56]. The entropic EPR steering criteria of Ref. [51] are likely to be useful in more complex scenarios.

In summary, if Charlie establishes that the statistics reported to him give an EPR paradox ($\mathrm{EPR}_{A|B} < 1$) *and* he trusts Alice's values, then he can be sure that there is genuine entanglement between the two observers. If his data fall in the region of entanglement but with no EPR paradox, he cannot be sure of this. The statistics could be consistent with a classical protocol, and the values x_A, p_A known to an infinite number of parties (Fig. 2).

VI. SECURITY AND THE MONOGAMY OF THE EPR PARADOX

In confirming an EPR paradox between Alice and Bob, Charlie can deduce the security of the amplitude values, based on a knowledge of quantum mechanics. As with Bell's nonlocality [10,57,58], the EPR paradox satisfies a very strict form of monogamy [39]. It is always true that (unless quantum mechanics fails or we cannot trust Alice's devices)

$$\mathrm{EPR}_{A|B}\mathrm{EPR}_{A|E} \geqslant 1, \tag{20}$$

where E is any other system measured by an eavesdropper Eve [35,38,39]. The monogamy relation (20) is derived based on the assumption of the uncertainty principle for $\hat{X}_A, \hat{P}_A$, and is one-sided DVI, that is, is valid no matter what devices or measurements are used by Bob, or Eve. Similarly to the relations introduced in Refs. [30,59], the mere measurement of $\mathrm{EPR}_{A|B}$ allows Charlie to deduce the level of security of the correlation between Alice's and Bob's amplitudes. If $\mathrm{EPR}_{A|B} < 1$ then $\mathrm{EPR}_{A|E} > 1$, and the conditional variances that give the noise levels on Eve's inferences of Alice's amplitudes is increased by an amount known to Charlie.

VII. DISCUSSION AND CONCLUSION

Here, we have demonstrated the principle of one-sided device-independent quantum security as applied to continuous variables. We believe this principle could expedite the practical application of device-independent cryptography and may lead to more secure protocols in CV quantum information.

We have shown that one-sided device-independent security is possible, using the widely available two-mode squeezed-state CV EPR source and quadrature phase amplitude measurements. The detection of entanglement via the EPR steering criterion is well documented in the literature and has been achieved without detection loopholes (though not as yet without locality loopholes). This quadrature amplitude EPR steering has been realized in a number of different optical scenarios [25,40,43,60,61], most of which are explained in the review of Ref. [26]. Also, more recently, very high degrees of EPR steering correlation have been reported [41]. It is significant for application to quantum communication protocols that the CV EPR steering criterion has been verified for pulses propagating through optical fibers [62], and has now been confirmed for spatially entangled optical modes and networks [63–65].

The biggest drawback to any practical implementation is the relative lack of robustness of the EPR paradox criterion to losses. It has been shown theoretically using monogamy relations that the criterion cannot be satisfied when there is 50% or more loss of the intensity received by the steering (untrusted) party [39]. For losses up to 50% on this channel, however, the criterion has been experimentally verified [40,43]. On the other hand, the criterion is quite robust with respect to the losses on the trusted party [40,53,54]. As detection can be done very efficiently using homodyne techniques, the greatest problem is likely to be the losses that enter on transmission. This may make the choice of location of the trusted and untrusted measurement stations important, as has been discussed in relation to applications of photonic steering [30,66]. All this gives promise to the prospect of utilizing CV one-sided device-independent witnesses for quantum information tasks.

It is stressed that two-sided device-independent entanglement witnesses could also be applied to CV scenarios. However, these may require more complicated measurements and protocols.

ACKNOWLEDGMENTS

This work was supported by the Australian Research Council Discovery Projects scheme, under grants DP130100949 and DP140104584. M.D.R. expresses thanks for the invitation to Ringberg Castle and the discussions held there.

[1] R. Gallego, L. E. Würflinger, A. Acín, and M. Navascués, Phys. Rev. Lett. **109**, 070401 (2012).
[2] A. Acin, N. Gisin, and L. Masanes, Phys Rev. Lett. **97**, 120405 (2006).
[3] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).
[4] J.-D. Bancal, N. Gisin, Y.-C. Liang, and S. Pironio, Phys. Rev. Lett. **106**, 250404 (2011).
[5] J.-D. Bancal, J. Barrett, N. Gisin, and S. Pironio, Phys. Rev. A **88**, 014102 (2013).
[6] T. Moroder, J.-D. Bancal, Y.-C. Liang, M. Hofmann, and O. Gühne, Phys. Rev. Lett. **111**, 030501 (2013).
[7] Y. Liu *et al.*, Phys. Rev. Lett. **111**, 130502 (2013).
[8] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175.
[9] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[10] V. Scarani and N. Gisin, Phys. Rev. Lett. **87**, 117901 (2001).
[11] J. Barrett, L. Hardy, and A. Kent, Phys. Rev. Lett. **95**, 010503 (2005).
[12] J. S. Bell, Physics (Long Island City, NY) **1**, 195 (1964); J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).
[13] M. Giustina *et al.*, Nature (London) **497**, 227 (2013); B. G. Christensen *et al.*, Phys. Rev. Lett. **111**, 130406 (2013).
[14] J. A. Larsson and J. Semitecolos, Phys. Rev. A **63**, 022117 (2001).
[15] X. Ma and N. Lütkenhaus, Quantum Inf. Comput. **12**, 203 (2012).
[16] C. Ci Wen Lim, C. Portmann, M. Tomamichel, R. Renner, and N. Gisin, Phys. Rev. X **3**, 031006 (2013).
[17] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, V. Scarani, V. Makarov, and C. Kurtsiefer, Phys. Rev. Lett. **107**, 170404 (2011).
[18] C. Weedbrook *et al.*, Rev. Mod. Phys. **84**, 621 (2012).
[19] T. C. Ralph, Phys. Rev. A **61**, 010303(R) (1999); M. D. Reid, *ibid.* **62**, 062308 (2000); Ch. Silberhorn, N. Korolkova, and G. Leuchs, Phys. Rev. Lett. **88**, 167902 (2002); F. Grosshans *et al.*, Nature (London) **421**, 238 (2003).
[20] F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner, Phys. Rev. Lett. **109**, 100502 (2012).
[21] V. Scarani *et al.*, Rev. Mod. Phys. **81**, 1301 (2009).
[22] M. Hillery, Phys. Rev. A **61**, 022309 (2000); L. S. Madsen, V. C. Usenko, M. Lassen, R. Filip, and U. L. Anderson, Nat. Commun. **3**, 1083 (2012); J. Leach, E. Bolduc, D. J. Gauthier, and R. W. Boyd, Phys. Rev. A **85**, 060304(R) (2012).
[23] A. Furusawa *et al.*, Science **282**, 706 (1998); W. P. Bowen, N. Treps, B. C. Buchler, R. Schnabel, T. C. Ralph, Hans-A. Bachor, T. Symul, and P. K. Lam, Phys. Rev. A **67**, 032302 (2003); T. C. Zhang, K. W. Goh, C. W. Chou, P. Lodahl, and H. J. Kimble, *ibid.* **67**, 033802 (2003); N. Takei *et al.*, Phys. Rev. Lett. **94**, 220502 (2005).
[24] S. Takeda *et al.*, Nature (London) **500**, 315 (2013); L. Steffen *et al.*, *ibid.* **500**, 319 (2013).
[25] Z. Y. Ou, S. F. Pereira, H. J. Kimble, and K. C. Peng, Phys. Rev. Lett. **68**, 3663 (1992).
[26] M. D. Reid *et al.*, Rev. Mod. Phys. **81**, 1727 (2009).
[27] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).
[28] M. D. Reid and P. D. Drummond, Phys. Rev. Lett. **60**, 2731 (1988).
[29] M. D. Reid, Phys. Rev. A **40**, 913 (1989).
[30] C. Branciard, E. G. Cavalcanti, S. P. Walborn, V. Scarani, and H. M. Wiseman, Phys. Rev. A **85**, 010301(R) (2012).
[31] H. M. Wiseman, S. J. Jones, and A. C. Doherty, Phys. Rev. Lett. **98**, 140402 (2007).
[32] S. J. Jones, H. M. Wiseman, and A. C. Doherty, Phys. Rev. A **76**, 052116 (2007).
[33] E. Schrödinger, Proc. Cambridge Philos. Soc. **31**, 555 (1935); **32**, 446 (1936).
[34] E. G. Cavalcanti, S. J. Jones, H. M. Wiseman, and M. D. Reid, Phys. Rev. A **80**, 032112 (2009).
[35] M. D. Reid, in *Quantum Squeezing*, edited by P. D. Drummond and Z. Ficek (Springer-Verlag, Berlin, 2004), p. 337.
[36] L. M. Duan, G. Giedke, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **84**, 2722 (2000).
[37] R. Simon, Phys. Rev. Lett. **84**, 2726 (2000).
[38] Q. Y. He and M. D. Reid, Phys. Rev. Lett. **111**, 250403 (2013).
[39] M. D. Reid, Phys. Rev. A **88**, 062108 (2013).
[40] W. P. Bowen, R. Schnabel, P. Lam, and T. C. Ralph, Phys. Rev. Lett. **90**, 043601 (2003).
[41] B. Hage, A. Samblowski, and R. Schnabel, Phys. Rev. A **81**, 062301 (2010); T. Eberle, V. Händchen, J. Duhme, T. Franz, R. F. Werner, and R. Schnabel, *ibid.* **83**, 052329 (2011); N. Takei, N. Lee, D. Moriyama, J. S. Neergaard-Nielsen, and

A. Furusawa, *ibid.* **74**, 060101(R) (2006); A. Samblowski *et al.*, in *Quantum Communication, Measurement and Computing*, edited by T. Ralph and P. K. Lam (AIP, New York, 2011), p. 219; S. Steinlechner, J. Bauchrowitz, T. Eberle, and R. Schnabel, Phys. Rev. A **87**, 022104 (2013).

[42] V. Giovannetti, S. Mancini, D. Vitali, and P. Tombesi, Phys. Rev. A **67**, 022320 (2003); S. Mancini, V. Giovannetti, D. Vitali, and P. Tombesi, Phys. Rev. Lett. **88**, 120401 (2002).

[43] D. Buono, G. Nocerino, A. Porzio, and S. Solimeno, Phys. Rev. A **86**, 042308 (2012).

[44] R. F. Werner, Phys. Rev. A **40**, 4277 (1989); A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).

[45] B. L. Schumaker and C. M. Caves, Phys. Rev. A **31**, 3093 (1985).

[46] E. P. Wigner, Phys. Rev. **40**, 749 (1932).

[47] J. S. Bell, *Speakable and Unspeakable in Quantum Mechanics* (Cambridge University Press, Cambridge, 1987).

[48] K. Banaszek and K. Wodkiewicz, Phys. Rev. A **58**, 4345 (1998).

[49] U. Leonhardt and J. Vaccaro, J. Mod. Opt. **42**, 939 (1995); A. Gilchrist, P. Deuar, and M. D. Reid, Phys. Rev. Lett. **80**, 3169 (1998).

[50] D. J. Saunders *et al.*, Nat. Phys. **6**, 845 (2010).

[51] S. P. Walborn, A. Salles, R. M. Gomes, F. Toscano, and P. H. Souto Ribeiro, Phys. Rev. Lett. **106**, 130402 (2011); J. Schneeloch, C. J. Broadbent, S. P. Walborn, E. G. Cavalcanti, and J. C. Howell, Phys. Rev. A **87**, 062103 (2013).

[52] A. J. Ferris, M. K. Olsen, E. G. Cavalcanti, and M. J. Davis, Phys. Rev. A **78**, 060104(R) (2008).

[53] S. L. W. Midgley, A. J. Ferris, and M. K. Olsen, Phys. Rev. A **81**, 022101 (2010).

[54] V. Händchen *et al.*, Nat. Photonics **6**, 598 (2012).

[55] K. Wagner *et al.*, arXiv:1203.1980.

[56] Q. Y. He and M. D. Reid, Phys. Rev. A **88**, 052121 (2013).

[57] B. Toner, Proc. R. Soc. London, Ser. A **465**, 59 (2009).

[58] Ll. Masanes, A. Acin, and N. Gisin, Phys. Rev. A **73**, 012112 (2006).

[59] M. Tomamichel and R. Renner, Phys. Rev. Lett. **106**, 110506 (2011).

[60] J. Laurat, T. Coudreau, G. Keller, N. Treps, and C. Fabre, Phys. Rev. A **71**, 022313 (2005).

[61] W. P. Bowen, N. Treps, R. Schnabel, and P. K. Lam, Phys. Rev. Lett. **89**, 253601 (2002).

[62] Ch. Silberhorn, P. K. Lam, O. Weiß, F. König, N. Korolkova, and G. Leuchs, Phys. Rev. Lett. **86**, 4267 (2001).

[63] K. Wagner, Science **321**, 541 (2008).

[64] V. Boyer *et al.*, Science **321**, 544 (2008).

[65] J. Roslund *et al.*, Nature Photonics **8**, 109 (2014).

[66] M. D. Reid, Phys. Rev. A **88**, 062338 (2013).