Versatility of continuous-variable asymmetric tripartite entanglement allows Alice and Clare to keep secrets from Bob

The versatility of continuous-variable asymmetric tripartite entanglement allows Alice and Clare to keep secrets from Bob

M. K. Olsen[1] and E. G. Cavalcanti[2]

[1]*School of Mathematics and Physics, University of Queensland, Brisbane, QLD 4072, Australia.*

[2]*Centre for Quantum Dynamics, Griffith University, Gold Coast, QLD 4215, Australia*

(Dated: November 6, 2018)

Abstract

The fully symmetric Gaussian tripartite entangled pure states will not exhibit two-mode Einstein Podolsky-Rosen (EPR)-steering. This means that any two participants cannot share quantum secrets using the security of one-sided device independent quantum key distribution (1SDI-QKD) without involving the third. They are restricted at most to standard quantum key distribution (S-QKD), which is less secure. Here we demonstrate an asymmetric tripartite system that can exhibit bipartite EPR-steering, so that two of the participants can use 1SDI-QKD without involving the other. This is possible because the promiscuity relations of continuous-variable tripartite entanglement are different from those of discrete-variable systems. We analyse these properties for two different systems, showing that the asymmetric system exhibits practical properties not found in the symmetric one.

PACS numbers: 42.50.-p,42.50.Dv,03.65.Ud,03.67.Dd

I. INTRODUCTION

Quantum key distribution (QKD) is the first mature technology which uses fundamental quantum mechanics [1], and allows for the creation of a secret key between authorised partners connected by a quantum channel and a classical authenticated channel. The field began with the presentation of the first complete protocol by Bennett and Brassard [2], based on ideas developed by Wiesner [3]. QKD can be performed with both discrete and continuous-variable systems and can be divided into three basic categories, with different security categorisations [4] and different degrees of quantum correlations needed to function effectively. The first of these is standard QKD (S-QKD), where both Alice and Bob trust their preparation and measurement devices, which requires only entanglement from the hierarchy defined by Wiseman *et al.* [5]. The second, known as one-sided device independent QKD (1SDI-QKD), only requires that one apparatus be trusted, and requires correlations at the level of Einstein-Podolsky-Rosen (EPR) [6] steering. The third, known as device independent QKD (DI-QKD) requires correlations at the level of Bell violations [7]. Here we analyse a feasible continuous-variable regime in which 1SDI-QKD is available between two participants in a fully tripartite entangled system, while the third cannot participate. Calling the participants Alice, Bob, and Clare, we show that for some systems Alice and Clare can exchange secret keys which are not accessible to Bob. We will also demonstrate that this is not possible in fully symmetric tripartite entangled systems.

Adesso *et al.* [8] have provided a classification scheme of continuous-variable Gaussian three-mode states with five distinct classes. The first classification describes states which are not separable under any of the three possible bipartitions. A subset of these states, which are invariant under the exchange of any two modes, are known as fully symmetric. Two examples of these are the states analysed by Aoki *et al.* [9], which mixes three squeezed states on two beamsplitters, and the triply concurrent downconversion scheme analysed by Smithers *et al.* [10] and Bradley *et al.* [11]. The fully symmetric states as defined by Adesso *et al.* [8] have the property that their covariance matrices can all be put in the same form by transformations which do not change the entanglement properties [12, 13], and Gaussian states have the property that they are completely characterised by the covariance matrix. This means that proving general properties of the fully symmetric states can be relatively simple. There are other possible tripartite Gaussian entangled states, one example of which

is produced by a scheme which combines downconversion and sum frequency generation [14–18], and does not possess the symmetry of the fully symmetric states. We will call this class of states asymmetric. Necessarily, these states will not have covariance matrices that can be put into an identical standard form. Any given asymmetric state will have a unique covariance matrix. This makes general proofs of the properties of asymmetric states more difficult, but as we merely wish to prove that something is possible, showing it for one member of the class of states is sufficient. We will show, that for the example of a fully tripartite entangled state considered here, 1SDI-QKD between two of the participants is indeed possible. As a demonstration of principle, we begin by examining a simple travelling wave model. We then analyse the appropriate correlation functions of the asymmetric scheme in the more experimentally relevant situation where the nonlinear medium is contained inside a pumped optical cavity.

II. ENTANGLEMENT AND EPR INEQUALITIES

With the annihilation operator $\hat{a}_i$ corresponding to mode i, we define the quadrature operators as $\hat{X}_i = \hat{a}_i + \hat{a}_i^\dagger$ and $\hat{Y}_i = -i(\hat{a}_i - \hat{a}_i^\dagger)$. The bipartite Einstein-Podolsky-Rosen (EPR) paradox [6] is detected by the well-known criteria developed by Reid [19], in terms of inferred quadrature variances,

$$\Pi V_{ij} = V^{inf}(\hat{X}_i)V^{inf}(\hat{Y}_i) \geq 1, \tag{1}$$

with an EPR state being indicated by violation of the inequality. This condition is optimal for bipartite Gaussian systems. Since this criterion was developed, Wiseman *et al.* [5] have formalised the concept of EPR-steering mathematically, showing that it is equivalent to the informal concept of steering developed by Schrödinger [20]. We will therefore refer to states which satisfy the criterion as possessing EPR-steering. In the above, ΠV_{ij} is the product of the inferred variances of mode i, as inferred by the operator with access to mode j. For pure Gaussian states and Gaussian measurements, such as those considered in the majority of this article, the Reid criterion is both necessary and sufficient to demonstrate EPR-steering [21].

Bipartite entanglement can be established in terms of the functions of quadrature variance inequalities developed by Duan and Simon [22, 23],

$$V(\hat{X}_i \pm \hat{X}_j) + V(\hat{Y}_i \mp \hat{Y}_j) \geq 4, \tag{2}$$

with violation of either of these being a demonstration of bipartite entanglement. We will call the first of these DS_{ij}^{+} and the second DS_{ij}^{-}. Because the travelling wave systems we consider are Gaussian and pure, these entanglement correlations are both necessary and sufficient for the demonstration of bipartite entanglement [24].

We will establish tripartite entanglement using the van Loock-Furusawa conditions [25], which give a set of three inequalities

$$V_{ij} = V(\hat{X}_i - \hat{X}_j) + V(\hat{Y}_i + \hat{Y}_j + g_k \hat{Y}_k) \geq 4, \tag{3}$$

for which the violation of any two demonstrates tripartite entanglement. The g_j, which are arbitrary and real, can be optimised [26], using the variances and covariances, as

$$g_i = -\frac{V(\hat{Y}_i, \hat{Y}_j) + V(\hat{Y}_i, \hat{Y}_k)}{V(\hat{Y}_i)}, \tag{4}$$

which is the process we follow here. Another set of inequalities was also presented by van Loock and Furusawa, the violation of any one of which is sufficient to prove tripartite entanglement,

$$V_{ijk} = V(\hat{X}_i - \frac{\hat{X}_j + \hat{X}_k}{\sqrt{2}}) + V(\hat{Y}_i + \frac{\hat{Y}_j + \hat{Y}_k}{\sqrt{2}}) \geq 4. \tag{5}$$

III. SYMMETRIC SYSTEMS

As our fully symmetric system, we will use the beamsplitter model of Aoki *et al.* [9], shown in Fig. 1. One of the pioneering systems for continuous variable tripartite entanglement, this came from van Loock and Braunstein [27], and was implemented experimentally by Aoki *et al.*, who mixed three squeezed states on two beamsplitters to obtain three entangled output beams. This setup is a subset of the systems recently analysed by Wang *et al.* [28]. The system uses three optical parametric oscillators (OPO), with the first, OPO_1, producing a state squeezed in the $\hat{Y}$ quadrature, while the other two produce $\hat{X}$ squeezed states. The annihilation operator $\hat{a}_j$ represents the output of OPO_j. The output of OPO_1 and OPO_2 are mixed on the first beamsplitter, BS_1, to produce outputs represented by $\hat{b}_0$ and $\hat{b}_1$. The field corresponding to $\hat{b}_0$ is then mixed with $\hat{a}_3$ on BS_2. The outputs of BS_2 are represented by $\hat{b}_2$ and $\hat{b}_3$. With the squeezed inputs, tripartite entanglement is found between the three outputs.

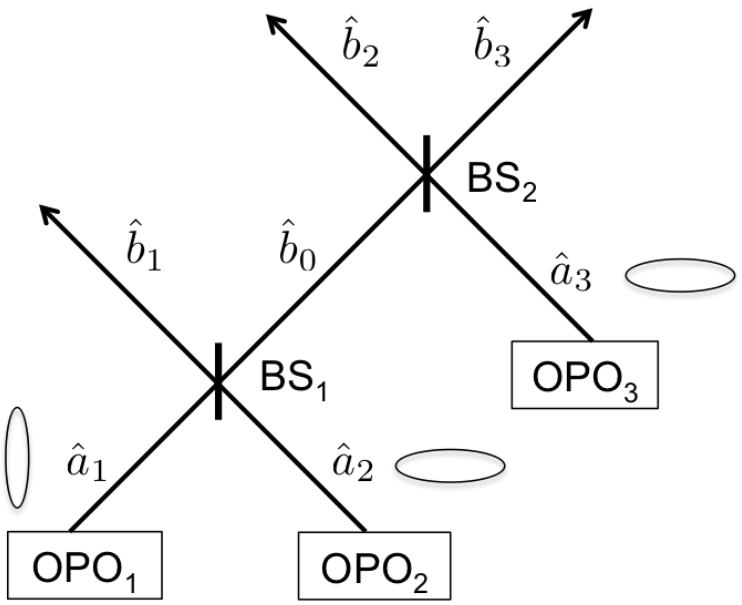

FIG. 1: The beam-splitter model used for symmetric systems. Three optical parametric oscillators produce outputs squeezed in the $\hat{Y}$ (OPO$_1$) or $\hat{X}$ (OPO$_2$ and OPO$_3$) quadratures. The outputs are combined with two beam-splitters, producing three output fields $\hat{b}_1, \hat{b}_2, \hat{b}_3$.

Assigning BS$_1$ a reflectivity of μ and BS$_2$ a reflectivity of ν, with $\mu = 2/3$ and $\nu = 1/2$ as in Aoki *et al.* [9] to give a fully symmetric state, we find the solutions for the $\hat{b}_j$ in terms of the inputs as

$$\begin{aligned}
\hat{b}_1 &= \sqrt{1-\mu}\,\hat{a}_1 + \sqrt{\mu}\,\hat{a}_2, \\
\hat{b}_2 &= \sqrt{\mu(1-\nu)}\,\hat{a}_1 - \sqrt{(1-\mu)(1-\nu)}\,\hat{a}_2 + \sqrt{\nu}\,\hat{a}_3, \\
\hat{b}_3 &= \sqrt{\mu\nu}\,\hat{a}_1 - \sqrt{\nu(1-\mu)}\,\hat{a}_2 - \sqrt{1-\nu}\,\hat{a}_3,
\end{aligned} \tag{6}$$

which allow us to find all the correlations we require for the bipartite and tripartite correlations we wish to calculate. The required variances and covariances are given in Ref. [29], and are all that is necessary to calculate the Duan-Simon, van Loock-Furusawa and EPR-steering correlations.

For a squeezing parameter r, we may assume minimum uncertainty squeezed input states (for more realistic inputs, see Ref. [29]) and set

$$\begin{aligned}
V(\hat{X}_{a_1}) &= V(\hat{Y}_{a_2}) = V(\hat{Y}_{a_3}) = \mathrm{e}^{r}, \\
V(\hat{Y}_{a_1}) &= V(\hat{X}_{a_2}) = V(\hat{X}_{a_3}) = \mathrm{e}^{-r},
\end{aligned} \tag{7}$$

which leads to the bipartite correlations of Eq. (2),

$$DS_{ij}^{\pm} = 4\cosh r \pm \frac{8}{3}\sinh r, \tag{8}$$

of which the DS_{ij}^{-} fall below 4 over a range of r. The inferred variances are found as

$$V^{inf}(\hat{X}_i) = \left[V^{inf}(\hat{Y}_i)\right]^{-1} = \frac{3\cosh r + \sinh r}{2 + \mathrm{e}^{2r}}, \tag{9}$$

so that the Reid EPR correlation of Eq. (1) is equal to unity for all r. We can also see that two-mode EPR is not possible for this system following the approach taken by Wang *et al.* [28]. Those authors considered the possibility of EPR-steering in the outputs of a cascading beamsplitter scheme of the type considered above, with N OPOs, $N-1$ beamsplitters, and N output modes, with the first OPO squeezed in the $\hat{X}$ quadrature and the remaining ones in the $\hat{Y}$ quadrature. If M of the output modes are used to steer any other of the output modes, EPR-steering can be demonstrated when the following function falls below one,

$$E_{i|M} = \frac{2(M+1)(N-M-1)[\cosh 4r - 1] + N^2}{2M(N-M)[\cosh 4r - 1] + N^2}\ . \tag{10}$$

In the case we consider, with $N = 3$ output modes it is easily seen that the above function is equal to 1 for $N = 3$ and $M = 1$, meaning that EPR-steering is not possible between any two of the output modes of the system above, for any value of the input squeezing parameters.

The optimised V_{ij} of Eq. (3) are found as

$$V_{ij} = \frac{2 + 10\mathrm{e}^{2r}}{\mathrm{e}^{r} + 2\mathrm{e}^{3r}}, \tag{11}$$

and the V_{ijk} of Eq. (5) are

$$V_{ijk} = 4\left(\cosh r - \frac{2\sqrt{2}}{3}\sinh r\right), \tag{12}$$

with these not changing under permutations of the indices. Note that, with optimisation, the V_{ij} begin at 4, rather than at the 5 found in Ref. [29] without optimisation. The uniqueness of the standard form of the covariance matrix for a pure fully symmetric Gaussian tripartite state, as shown by Adesso *et al.* [8], means that all possible symmetric Gaussian three-mode systems have a covariance matrix which can be written in the same form. This means that Eq. (9) shows that bipartite EPR-steering is not possible in any fully symmetric Gaussian tripartite system. This result shows that at most S-QKD is possible between any pair of

Alice, Bob, and Clare with this system. All three must participate in any device independent QKD. Although not shown here, the violation of three-mode EPR-steering correlations [29] for this system shows that the participants can combine pairwise to perform 1SDI-QKD with the third participant [30].

IV. AN ASYMMETRIC SYSTEM

Our asymmetric system, which combines downconversion with sum-frequency generation, was first proposed by Smithers and Lu [10], and theoretically analysed in a travelling wave configuration by Ferraro *et al.* [15], and in an intracavity configuration by Yu *et al.* [16]. The configuration was subsequently analysed in more depth by Pennarun *et al.* [18], who investigated the stability properties and predicted tripartite entanglement in different regimes. It consists of a nonlinear medium pumped at frequency ω_0. The downconversion part of the process, denoted by the effective nonlinearity κ_1, generates two fields at ω_1 and ω_3, where $\omega_0 = \omega_1 + \omega_3$. The pump field at ω_0 can then combine with the field at ω_3 in a sum frequency generation process [32], to produce a further field at ω_2, with effective nonlinearity κ_2. We will use the annihilation operators $\hat{a}_j$ to describe the fields at ω_j for $j = 1, 2, 3$. If we consider that the pump field is intense and classical so that depletion does not become important, we may write the interaction Hamiltonian as

$$\mathcal{H}_{int} = i\hbar\kappa_1(\hat{a}_1^\dagger\hat{a}_3^\dagger - \hat{a}_1\hat{a}_3) + i\hbar\kappa_2(\hat{a}_3\hat{a}_2^\dagger - \hat{a}_3^\dagger\hat{a}_2). \tag{13}$$

In what follows we will define the variable ζ as $\kappa_1^2 - \kappa_2^2$.

We find that the Heisenberg equations of motion for the annihilation and creation operators, being linear, may be solved analytically after Jordan decomposition of the time evolution matrix, as described in standard undergraduate textbooks [31]. We used Mathematica for this, allowing us to write solutions for the quadrature operators (noting that

$\kappa_1 > \kappa_2$ here),

$$\begin{aligned}
\hat{X}_1(t) &= \frac{\kappa_1^2\cosh\zeta t - \kappa_2^2}{\zeta^2}\hat{X}_1(0) - \frac{\kappa_1\kappa_2(\cosh\zeta t - 1)}{\zeta^2}\hat{X}_2(0) + \frac{\kappa_1\sinh\zeta t}{\zeta^2}\hat{X}_3(0),\\
\hat{X}_2(t) &= \frac{\kappa_1\kappa_2(\cosh\zeta t - 1)}{\zeta^2}\hat{X}_1(0) + \frac{\kappa_1^2 - \kappa_2^2\cosh\zeta t}{\zeta^2}\hat{X}_2(0) + \frac{\kappa_1\sinh\zeta t}{\zeta^2}\hat{X}_3(0),\\
\hat{X}_3(t) &= \frac{\kappa_1\sinh\zeta t}{\zeta^2}\hat{X}_1(0) - \frac{\kappa_2\sinh\zeta t}{\zeta^2}\hat{X}_2(0) + \cosh\zeta t\ \hat{X}_3(0),\\
\hat{Y}_1(t) &= \frac{\kappa_1^2\cosh\zeta t - \kappa_2^2}{\zeta^2}\hat{Y}_1(0) + \frac{\kappa_1\kappa_2(\cosh\zeta t - 1)}{\zeta^2}\hat{Y}_2(0) - \frac{\kappa_1\sinh\zeta t}{\zeta^2}\hat{Y}_3,\\
\hat{Y}_2(t) &= -\frac{\kappa_1\kappa_2(\cosh\zeta t - 1)}{\zeta^2}\hat{Y}_1(0) + \frac{\kappa_1^2 - \kappa_2^2\cosh\zeta t}{\zeta^2}\hat{Y}_2(0) + \frac{\kappa_1\sinh\zeta t}{\zeta^2}\hat{Y}_3(0),\\
\hat{Y}_3(t) &= -\frac{\kappa_1\sinh\zeta t}{\zeta^2}\hat{Y}_1(0) - \frac{\kappa_2\sinh\zeta t}{\zeta^2}\hat{Y}_2(0) + \cosh\zeta t\ \hat{Y}_3(0),
\end{aligned} \tag{14}$$

which allows us to find expressions for all the entanglement and EPR-steering correlations. Setting

$$\begin{aligned}
\alpha &= \frac{\kappa_1^2\cosh\zeta t - \kappa_2^2}{\zeta^2},\\
\beta &= \frac{\kappa_1\kappa_2(\cosh\zeta t - 1)}{\zeta^2},\\
\gamma &= \frac{\kappa_1\sinh\zeta t}{\zeta^2},\\
\delta &= \frac{\kappa_1^2 - \kappa_2^2\cosh\zeta t}{\zeta^2},\\
\epsilon &= \frac{\kappa_2\sinh\zeta t}{\zeta^2},\\
\eta &= \cosh\zeta t,
\end{aligned} \tag{15}$$

and noting that the single quadrature expectation values vanish when the input modes are

vacuum, we find the moments required for the variances and covariances as

$$\begin{aligned}
\langle \hat{X}_1^2 \rangle &= \langle \hat{Y}_1^2 \rangle = \alpha^2 + \beta^2 + \gamma^2, \\
\langle \hat{X}_2^2 \rangle &= \langle \hat{Y}_2^2 \rangle = \beta^2 + \delta^2 + \gamma^2, \\
\langle \hat{X}_3^2 \rangle &= \langle \hat{Y}_3^2 \rangle = \gamma^2 + \epsilon^2 + \eta^2, \\
\langle \hat{X}_1 \hat{X}_2 \rangle &= \alpha\beta - \beta\delta + \gamma^2, \\
\langle \hat{X}_1 \hat{X}_3 \rangle &= \alpha\gamma + \beta\epsilon + \gamma\eta, \\
\langle \hat{X}_2 \hat{X}_3 \rangle &= \gamma\beta - \delta\epsilon + \gamma\eta, \\
\langle \hat{Y}_1 \hat{Y}_2 \rangle &= -\alpha\beta + \beta\delta - \gamma^2, \\
\langle \hat{Y}_1 \hat{Y}_3 \rangle &= -\alpha\gamma - \beta\epsilon - \gamma\eta, \\
\langle \hat{Y}_2 \hat{Y}_3 \rangle &= \beta\gamma - \delta\epsilon + \gamma\eta.
\end{aligned} \tag{16}$$

Setting $\kappa_2 = 0.6\kappa_1$, we find that the correlation V_{123} is the most sensitive for the detection of tripartite entanglement, as shown in Fig. 2. According to Eq. (5), this correlation being less than four is sufficient to demonstrate that the system exhibits full tripartite entanglement. We find that only one of the possible bipartitions exhibits bipartite entanglement, with this being shown by DS_{13}^{-} of Eq. (2). None of the other bipartitions were found to violate the necessary inequalities and have not been shown here. We also see, in Fig. 3, that there is bipartite EPR-steering between modes 1 and 3, with the expressions needed for the correlations of Eq. (1) given by

$$\begin{aligned}
\Pi V_{13} &= \frac{\left[(\alpha^2 + \beta^2 + \gamma^2)(\gamma^2 + \epsilon^2 + \eta^2) - (\alpha\gamma + \beta\epsilon + \gamma\eta)^2\right]^2}{(\gamma^2 + \epsilon^2 + \eta^2)^2}, \\
\Pi V_{31} &= \frac{\left[(\alpha^2 + \epsilon^2 + \eta^2)(\beta^2 + \gamma^2 + \delta^2) - (\alpha\gamma + \beta\epsilon + \gamma\eta)^2\right]^2}{(\beta^2 + \delta^2 + \gamma^2)^2},
\end{aligned} \tag{17}$$

where the regimes where these expressions fall below unity then best seen by plotting of the analytical results. We find that no EPR-steering is possible between any of the other pairs. The EPR-steering between Alice and Clare is almost symmetric for the input parameters used here, although asymmetric EPR-steering [33] can be seen for other parameters. As we have assigned modes to Alice, Bob, and Clare in numerical order, this means that there is a possibility that Alice and Clare can share secrets using 1SDI-QKD, without involving Bob. Bob cannot even participate in S-QKD with either of the other two. This feature is a direct result of the promiscuity of asymmetric continuous-variable tripartite entanglement, and is

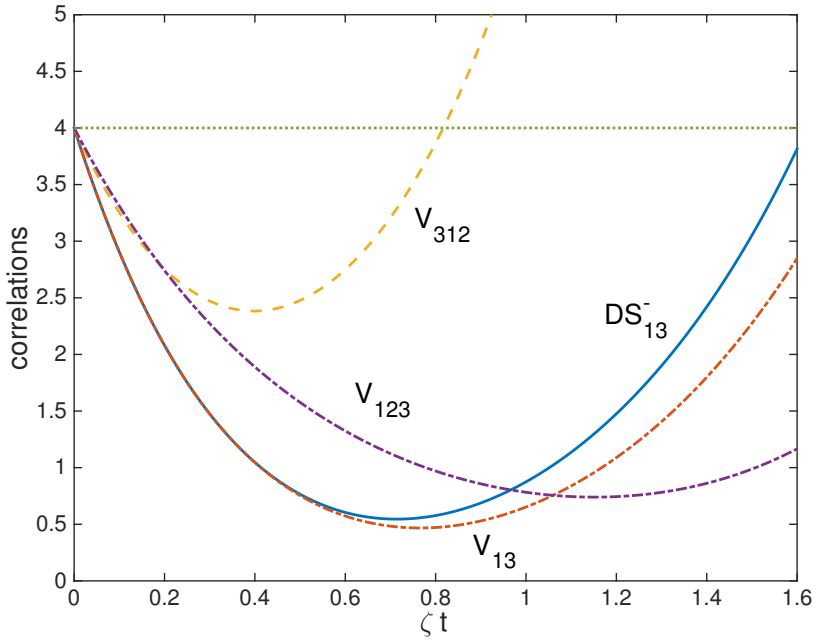

FIG. 2: (colour online) DS_{13}^{-}, V_{123}, V_{312}, and V_{13} for the asymmetric model, with $\kappa_2 = 0.6\kappa_1$. We see that both bipartite and tripartite entanglement are predicted over a range of interaction strength ζt. Note that the line at 4 is a guide to the eye.

a demonstration of the flexibility of continuous-variable systems. When we examine [30] the tripartite EPR-steering correlations of Ref. [29], we find that Bob and Clare together can steer Alice, while Alice and Bob together only violate the necessary inequality marginally. Alice and Clare together cannot steer Bob at all for the parameters used here.

To ensure that 1SDI-QKD is in fact viable between Alice and Clare, we also need to calculate the bit rate. As shown in [4], EPR-steering is necessary, but not sufficient for 1SDI-QKD. The continuous-variable case was analysed by Walk *et al.* [34]. In their work, the secret key is encoded in the $\hat{X}$ quadrature of a field mode j, and a sufficiently strong demonstration of CV EPR-steering from mode i to j bounds the information that an eavesdropper can have about the key, in a way that is independent of the device at mode i, so that a secret key rate obtained using reverse reconciliation is lower bounded by

$$K_{min} \geq \log\left(\frac{2\mathrm{e}^{-1}}{\sqrt{\Pi V_{ij}}}\right). \tag{18}$$

As long as this minimum rate is positive, 1SDI-QKD is possible. Eq. (18) implies that a positive key rate is achievable for $\Pi V_{ij} < (2/e)^2$, compared to $\Pi V_{ij} < 1$ for EPR-steering.

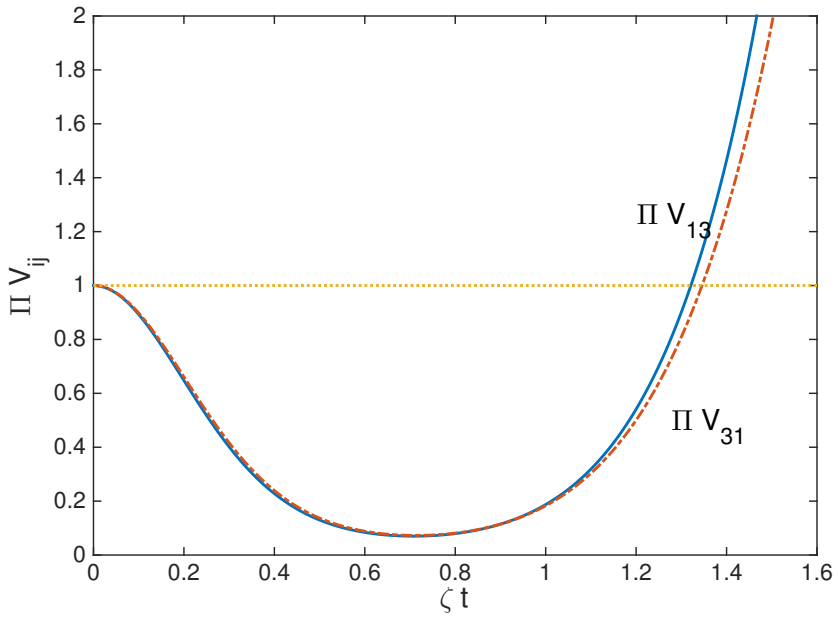

FIG. 3: (colour online) The EPR-steering correlations for modes 1 and 3 of the asymmetric model, with $\kappa_2 = 0.6\kappa_1$. Note that the line at 1 is a guide to the eye.

Fig. 4 shows that in this asymmetric scheme the key rate is indeed positive between Alice and Clare over the parameter range $0.248 < \zeta t < 1.216$ for Alice steering Clare (i.e. the protocol being device-independent for Alice) and $0.240 < \zeta t < 1.216$ for Clare steering Alice, and negative for any pair-wise coupling in the symmetric scheme.

V. INTRACAVITY RESULTS

Having examined the asymmetric model using the solution of the Heisenberg equations of motion, which give a proof of principle, we now turn to the more experimentally realistic case where the nonlinear medium is housed inside a pumped optical cavity. With the cavity pumping field denoted by ϵ, and the cavity loss rate for mode j denoted by γ_j (with γ_0 being the loss rate at the pump frequency), and again with $\kappa_2 = 0.6\kappa_1$, the critical pump value for the oscillation threshold is found as [18]

$$\epsilon_c = \frac{\gamma_0\sqrt{\gamma_1\gamma_2\gamma_3}}{\sqrt{\kappa_1^2\gamma_2 - \kappa_2^2\gamma_1}}. \tag{19}$$

For pump values below this, we may linearise the equations of motion and treat the system as an Ornstein-Uhlenbeck process [35], which allows us to calculate in intracavity spectral

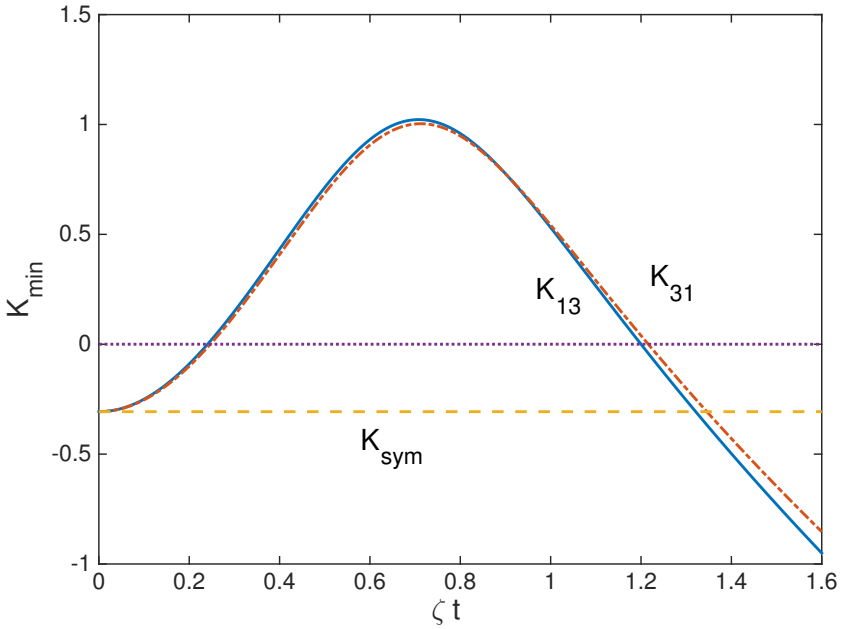

FIG. 4: (colour online) The minimum bit rates for modes 1 and 3 of the asymmetric model, with $\kappa_2 = 0.6\kappa_1$, and the minimum rate for any pair of the symmetric scheme. K_{ij} is the minimum bit rate for mode j sending a quantum key to mode i. A positive value shows that 1SDI-QKD is possible. The line at zero is a guide to the eye.

variances as in Eq. (11) of Pennarun *et al.* [18]. Along with the input-output relations developed by Gardiner and Collett [36], this allows for easy calculation of output spectral correlations as a function of ω $(= \gamma_1)$, the frequency from the cavity resonance. Although analytical results are also possible here, they become rather unwieldy, so we will present numerical results for the correlations of interest in this section. In the results presented, we use the numerical parameter values $\gamma_0 = \gamma_1 = \gamma_3 = 1$, $\gamma_2 = 3\gamma_0$, and $\kappa_1 = 0.01$.

In Fig. 5 we show the spectral output results for the bipartite EPR-steering correlations which show a value of less than one, for $\epsilon = 0.8\epsilon_c$. The steering results for Alice and Clare are very close to symmetric. We also see that Alice can steer Bob to some extent, a feature which was not evident in our travelling wave model. However, this does not allow Bob to participate in 1SDI-QKD, as shown in Fig. 6, where we see that the minimum bit rate between Alice and Bob is not positive. Our predictions from the simpler model are still reliable. We also see that, as expected, the useable bandwith for 1SDI-QKD is narrower than that for EPR-steering. Since there is often excess noise in the vicinity of zero frequency,

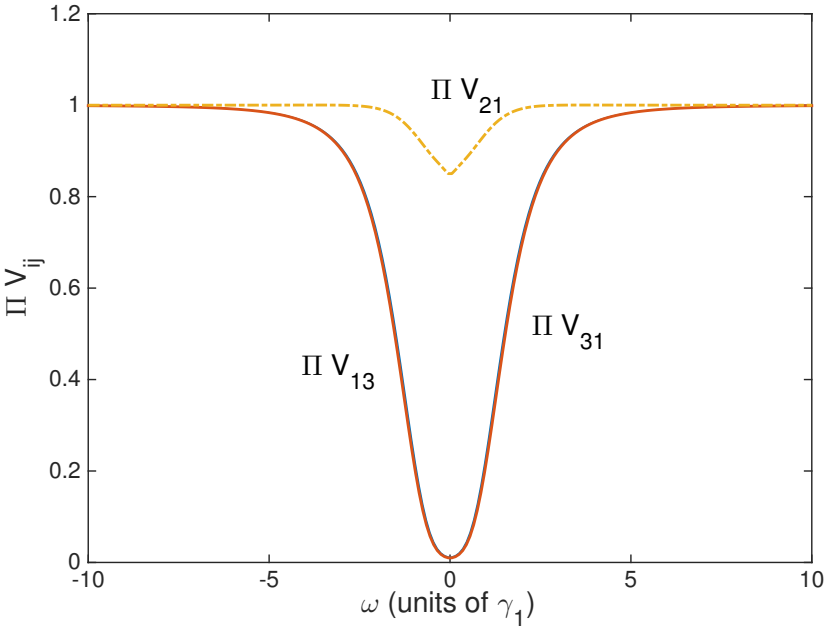

FIG. 5: (colour online) The output spectral EPR-steering correlations for $\epsilon = 0.8\epsilon_c$. We see that Bob can now be steered by Alice, although the violation of the inequality is much less than those for Alice and Clare. ω represents the frequency in terms of γ_1 around the cavity resonance.

the bandwidth is an operationally important feature. Fig. 7 shows the minimum bit rates as a function of ϵ/ϵ_c over the range $0.1\epsilon_c \leq \epsilon \leq 0.98\epsilon_c$, with all other parameters as in the previous two figures. We again see that Alice and Clare enjoy a level of security that is not available to Bob, over this whole range.

VI. CONCLUSIONS

We have studied the entanglement properties of an asymmetric tripartite system produced by combining downconversion with sum-frequency generation, finding that it offers an extra degree of flexibility over fully symmetric ones for QKD. With the three participants labelled as Alice, Bob, and Clare, we have shown that any pairing can share secrets using S-QKD in symmetric systems, with bipartite entanglement being available over a range of the interaction parameter. There is no bipartite 1SDI-QKD possible in these systems, with all three participants needing to be involved for the level of communication security provided by this method. On the other hand, the asymmetric system analysed here allows both bipartite

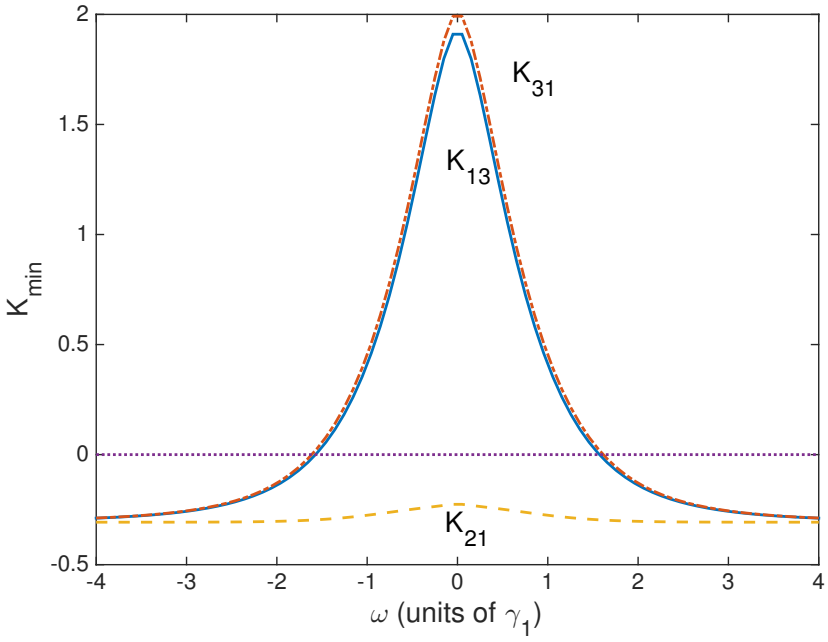

FIG. 6: (colour online) The spectral minimum bit rates for Alice sending a quantum key to Bob, and Alice and Clare sending to each other. A positive value shows that 1SDI-QKD is possible. Note that the frequency axis is narrower than for Fig. 5, reflecting the fact that the bandwidth for 1SDI-QKD is less tha that for EPR-steering. The line at zero is a guide to the eye.

S-QKD and 1SDI-QKD, with Bob only being able to participate in tripartite S-QKD. In the symmetric system, any pair of participants can also steer the remaining participant, which means that tripartite 1SDI-QKD is available as long as they work in pairs. This is not the case in the asymmetric system. In conclusion, we have shown that asymmetric Gaussian systems can offer a level of flexibility to quantum key distribution that is not available with fully symmetric systems. This may well be advantageous for some applications, for example where different levels of security are desired within a network.

Acknowledgments

This research was supported by the Australian Research Council under the Future Fellowships Program (Grant ID: FT100100515). MKO acknowledges invaluable discussions with Joel Corney.

[1] V. Scarani, H. Bechmann-Pasquinucci, N.J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev,

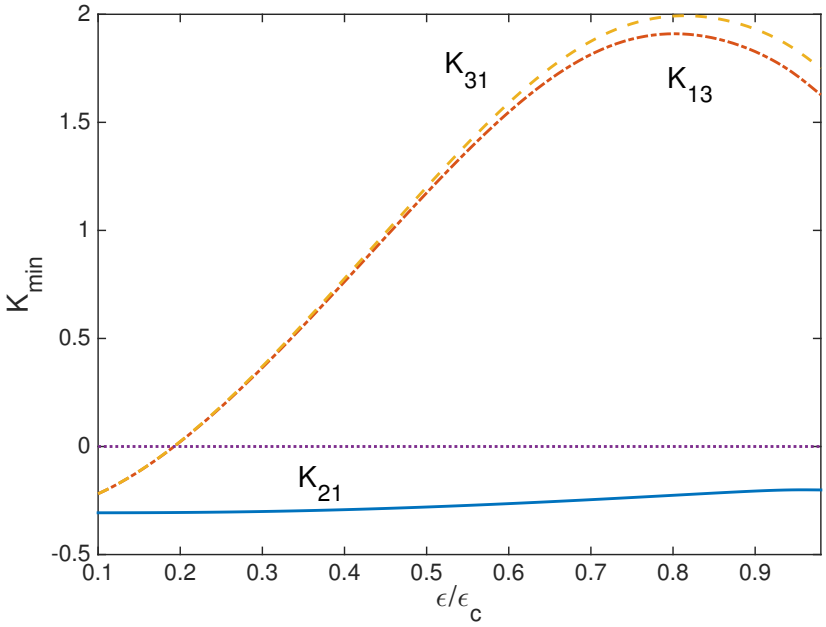

FIG. 7: (colour online) The minimum bit rates for modes 1 and 3 of the asymmetric model, with $\kappa_2 = 0.6\kappa_1$, and the minimum rate for any pair of the symmetric scheme. K_{ij} is the minimum bit rate for mode j sending a quantum key to mode i. A positive value shows that 1SDI-QKD is possible. The line at zero is a guide to the eye.

Rev. Mod. Phys. **81**, 1301 (2009).

[2] C.H. Bennett and G. Brassard, *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York) 1984.

[3] S. Wiesner, SIGACT News **15**, (1983).

[4] C. Branciard, E.G. Cavalcanti, S.P. Walborn, V. Scarani, and H.M. Wiseman, Phys. Rev. A **85**, 010301 (2012).

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

[6] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1937).

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

[8] G. Adesso, A. Serafini, and F. Illuminati, Phys. Rev. A **73**,032345 (2006).

[9] T. Aoki, N. Takei, H. Yonezawa, K. Wakui, T. Hiraoka, A. Furusawa, and P. van Loock, Phys. Rev. Lett. **91**, 080404 (2003).

[10] M.E. Smithers and E.Y.C. Lu, Phys. Rev. A **10**, 1874 (1974).

[11] A.S. Bradley, M.K. Olsen, O. Pfister and R.C. Pooser, Phys. Rev. A **72**, 053805 (2005).

[12] A. Serafini, G. Adesso, and F. Illuminati, Phys. Rev. A **71**, 032349 (2005).

[13] G. Adesso, A. Serafini, and F. Illuminati, Phys. Rev. Lett. bf 93, 220504 (2004).

[14] B. Fortescue and H.-K. Lo, Phys. Rev. Lett. **98**, 260501 (2007).

[15] A. Ferraro, M.G.A. Paris, M. Bondani, A. Allevi, E. Puddu, and A. Andreoni, J. Opt. Soc. Am. B **6**, 1241 (2004).

[16] Y.B. Yu, Z.D. Xie, X.Q. Yu, H.X. Li, P. Xu, H.M. Yao, and S.N. Zhu, Phys. Rev. A **74**, 042332 (2006).

[17] M.K. Olsen and A.S. Bradley, J. Phys. B **39**, 127 (2006).

[18] C. Pennarun, A.S. Bradley, and M.K. Olsen, Phys. Rev. A **76**, 063812 (2007).

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

[20] E. Schrödinger, Proc. Cam. Philos. Soc. **31**, 555 (1935).

[21] S.J. Jones, H.M. Wiseman, and A.C. Doherty, Phys. Rev. A **76**, 052116 (2007).

[22] L.-M. Duan, G. Giedke, J.I. Cirac and P. Zoller, Phys. Rev. Lett. **84**, 2722 (2000).

[23] R. Simon, Phys. Rev. Lett. **84**, 2726 (2000).

[24] R.Y. Teh and M.D. Reid, Phys. Rev. A **90**, 062337 (2014).

[25] P. van Loock and A. Furusawa, Phys. Rev. A **67**, 052315 (2003).

[26] M.K. Olsen and A.S. Bradley, Phys. Rev. A **74**, 063809 (2006).

[27] P. van Loock and S.L. Braunstein, Phys. Rev. Lett. **84**, 3482 (2000).

[28] M. Wang, Y. Xiang, Q. He, and Q. Gong, Phys. Rev. A **91**, 012112 (2015).

[29] M.K. Olsen, A.S. Bradley and M.D. Reid, J. Phys. B **39** 2515 (2006).

[30] M.K. Olsen and J.F. Corney, to be submitted soon.

[31] G. Teschl, *Ordinary Differential Equations and Dynamical Systems*, (American Mathematical Society, Providence, 2012.)

[32] M.K. Olsen and A.S. Bradley, Phys. Rev. A **77**, 023813 (2008).

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

[34] N. Walk, H.M. Wiseman, and T.C. Ralph, arXiv:1405.6593v2.

[35] C.W. Gardiner, *Handbook of Stochastic Methods*, (Springer, Berlin, 1985.)

[36] C.W. Gardiner and M.J. Collett, Phys. Rev. A **31**, 3761 (1985).