Quantum Inf Process
DOI 10.1007/s11128-015-1063-4

Coherent state quantum key distribution based on entanglement sudden death

Gregg Jaeger[1] · **David Simon**[2,3] · **Alexander V. Sergienko**[3,4]

Received: 25 June 2015 / Accepted: 27 June 2015

Abstract A method for quantum key distribution (QKD) using entangled coherent states is discussed which is designed to provide key distribution rates and transmission distances surpassing those of traditional entangled photon pair QKD by exploiting entanglement sudden death. The method uses entangled electromagnetic signal states of 'macroscopic' average photon numbers rather than single photon or entangled photon pairs, which have inherently limited rate and distance performance as bearers of quantum key data. Accordingly, rather than relying specifically on Bell inequalities as do entangled photon pair-based methods, the security of this method is based on entanglement witnesses and related functions.

Keywords Quantum key distribution · Entanglement sudden death · Entanglement witness · Entanglement · Coherent states · Quantum cryptography · Eavesdropping detection

1 Introduction

Advanced quantum key distribution (QKD) is the distribution of random, shared encryption key material between two or more parties using quantum physical sig-

✉ Gregg Jaeger
jaeger@bu.edu

1 Quantum Communication and Measurement Laboratory, Division of Natural Science and Mathematics, Department of Electrical and Computer Engineering, Boston University, Boston, MA 02215, USA

2 Department of Physics and Astronomy, Stonehill College, 320 Washington Street, Easton, MA 02357, USA

3 Department of Electrical and Computer Engineering, Boston University, 8 Saint Marys Street, Boston, MA 02215, USA

4 Department of Physics, Boston University, 590 Commonwealth Avenue, Boston, MA 02215, USA

Published online: 16 July 2015

nals, with the security of the distribution based on the fundamental laws of quantum theory [1]. The original methods for performing QKD were based on low-intensity light signals, something which makes the presence of eavesdropping easy to detect due to the relatively large disturbance that any quantum measurement will have on such states when the details of state preparation—for example, the elements of the basis in which the pure state density matrix of the signal states is diagonal—are unknown to the eavesdropper. In basic QKD protocols, two participants—conventionally referred to as Alice and Bob—generate a shared binary encryption key in such a way that an eavesdropper, called Eve, cannot obtain useful knowledge regarding the key without being detectable. In this way, communication system security is greatly strengthened beyond what traditional, classical cryptographic methods can offer. However, the efficiencies and effective distances of QKD schemes based on low-intensity signals—for example, those using single photons or entangled photon pairs—are limited by the relative ease with which individual photons are lost to the environment, because such losses have a great effect on the signal state. The use of higher intensity signals is an obvious alternative, but one which must similarly ensure that any eavesdropping be detectable. Here, such an alternative is pursued in a system using entangled coherent states of light.

Although the use of entanglement offers specific technical advantages to any QKD system, entanglement sudden death (ESD), the loss of entanglement in finite times and distances, has the potential to threaten QKD system integrity, particularly in few photon level-based systems. For this reason, we recently addressed this threat from a theoretical point of view in the realm of low photon number systems, for overcoming the threat of ESD through the use of decoherence free subspaces (DFSs) and related techniques; we showed that, although this threat can be mitigated in some cases, it cannot always be overcome in the low-intensity QKD context [2,3]. Fortunately, this threat is far less pronounced at high intensities and can even be used to advantage. Here, we discuss such an entangled coherent state approach to QKD, which, because it is not based on low-intensity signals, does not involve a design based on DFSs to resist ESD, but rather has the capacity to *exploit* ESD to provide security against eavesdropping [4].

We show here that one may overcome the limitations of the above-mentioned shortcomings of single photon-based or photon pair-based methods by using pairs of entangled *coherent states* of the quantum electromagnetic field. Greater efficiency and transmission distances can be achieved with such states because coherent states are robust to partial beam loss. Not unexpectedly, large effective distances and relatively high transmission rates come at some cost to security: Eavesdropping can be more difficult to detect because even a small portion of the signal beam can be useful in obtaining knowledge of the states being exchanged by those attempting to share a secure string of cryptographic key bits. Creating the required entangled coherent states [5,6] is also a greater challenge than creating entangled photon pairs, which can be done efficiently using quantum parametric down-conversion, cf. [7]. However, the latter problem is only one of current practice, not one of principle or foreseeable practice. A number of QKD methods based on the use of coherent states have been proposed, but fewer have been based on the use of entangled coherent states. The spe-

cific method offered here is the entangling of a pair of coherent states via a conditional nonlinear interaction with auxiliary single photons [8].

2 Phase-entangling coherent states and encoding key bit values

In order to produce an entangled state of two electromagnetic field modes involving just a single photon, such as

$$\frac{1}{\sqrt{2}}\left(|0\rangle|1\rangle + \mathrm{e}^{i\phi}|1\rangle|0\rangle\right), \tag{1}$$

a single beam splitter and a photon will suffice. In the case where one desires to produce an entangled state of two *coherent states* of these modes, more is required [9]. A relatively simple approach is that of the QKD signal state preparation of [8], in which a beam splitter is used to prepare a single photon in a spatial path state superposition in only one of which will the nonlinear interaction, such as that involving the Kerr effect, be able to take place with each of two coherent states in any complete process; this then prepares a phase-entangled coherent state QKD signal state, the phase of which can be measured through homodyning.

A general Kerr interaction between a photon number eigenstate of the electromagnetic field and a coherent state can be described as follows. This interaction coupling of strength χ can be described by the Hamiltonian $H = -\hbar\chi a_1^\dagger a_1 a_2^\dagger a_2$, so that the interaction of a mode in the Fock state $|n\rangle$ with a mode in the coherent state $|\alpha\rangle$ is given by $\mathrm{e}^{i\hbar HT}|\alpha\rangle|n\rangle = |\alpha\mathrm{e}^{in\theta}\rangle|n\rangle$, where α is a complex number providing the complex state amplitude corresponding to a distribution over particle number; the resulting phase shift θ on the coherent state is determined by χ and by the interaction time T.

In the situation of interest here, that in which the entangled coherent state is prepared in the laboratory of the sender, Alice, entangled coherent state preparation proceeds as follows. As illustrated in Fig. 1, a coherent state produced by a laser is directed to

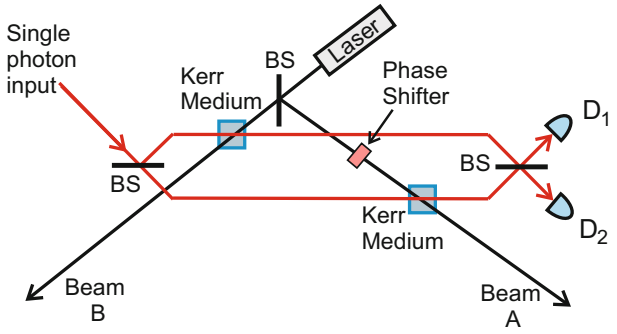

Fig. 1 (Color online) State preparation for a user-symmetric coherent state key distribution system with entanglement prepared by single photon inputs via the Kerr effect. An initial beam splitter splits an initial coherent states beam into two equal-amplitude states, while single photons enter a superposition of two paths on a second beam splitter, resulting in a superposition of two coherent state joint states having opposite phase shifts

a beam splitter, which produces a pair of coherent states $|\alpha\rangle$ in two distinct beams. The states of these beams are then entangled by a possible nonlinear interaction of each of them conditionally to a single photon (as described, for example, in Ref. [8]), a different beam splitter having put the photon into a superposition, such as that of Eq. 1, of two paths of a Mach–Zehnder-type interferometer within Alice's laboratory. Thus, if the photon were to follow the upper path, then the coherent state of beam B is phase shifted by 2ϕ due to cross-phase modulation of the photon with the beam in a nonlinear medium, such as a Kerr medium, for example [10–15]; if the photon were to take the lower path, the coherent state in Beam A would be phase shifted by 2ϕ. Adding a constant phase shift of ϕ to both beams will then result in the sort of entangled output state desired:

$$|\psi\rangle = \frac{N}{\sqrt{2}}\left(|\alpha_+\rangle|\beta_-\rangle + \mathrm{e}^{i\theta}|\alpha_-\rangle|\beta_+\rangle\right), \tag{2}$$

where $\alpha_\pm \equiv \alpha \mathrm{e}^{\pm i\phi}$, $\beta_\pm \equiv \beta \mathrm{e}^{\pm i\phi}$, and $|N|^2 = \left(1 + \cos\theta\ \mathrm{e}^{-4\alpha^2 \sin^2\phi}\right)^{-1}$, the single photon states not being explicitly described here for simplicity of illustration. Note that, $\pm\phi$ are the phase shifts of the coherent states, whereas θ is simply the single photon state phase as determined by the photon's trajectory. By keeping only those events in which the photon is detected at D_1, one has $\theta = \pi$; for those events in which it exits at D_2, one has instead $\theta = 0$. (If other values of θ were desired, one could simple increase the effective path difference, for example, by placing glass in one of the paths.)

The approach to QKD described here can be seen to use a method for entangled coherent state preparation similar to that offered in [8]. However, the method of eavesdropping detection used there, namely based on testing for a Bell-type inequality violation, is rather inefficient. Therefore, we instead base our approach on a related but much more efficiently measured quantity, namely an entanglement witness, cf. [16,17]. Entanglement, being a weaker property than Bell violation, has the potential to increase the allowed operating distance for the QKD system we describe here. Entanglement is tested by measuring the value of the witness, something in the simplest case readily done through basic homodyne measurements. An apparatus for implementing the entangled coherent state quantum key distribution method is shown in Fig. 2, below. By making homodyne measurements, Alice and Bob can each measure the phase of the state in their respective beams. Since the shifts in the two beams are always opposite in sign, Alice and Bob can readily use the relative sign of their measured shifts to obtain the desired common key. Thus, for example, when Alice finds $-\phi$ and Bob finds $+\phi$, the two can follow the convention that this indicates a shared common bit value of 1 and in the alternative case where the signs of the two phases are exchanged, take this to indicate the bit value 0.

3 Effect of noise on entangled coherent states

The primary noise mechanism (and eavesdropping effect) acting on the entangled coherent states in the environment that must be taken into account is the loss of

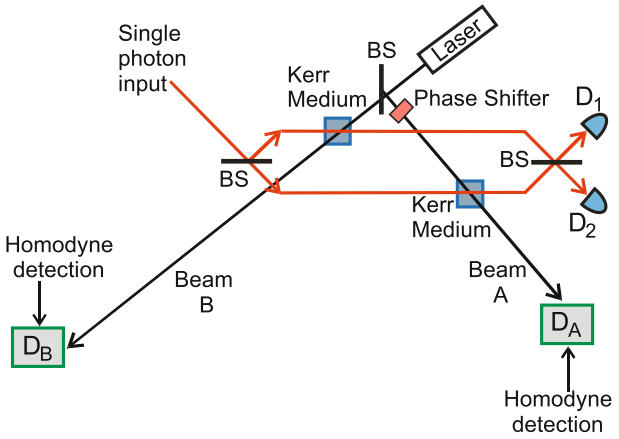

Fig. 2 (Color online) An apparatus for implementing the entangled coherent state quantum key distribution method described here. After state preparation by the apparatus of the previous figure, the users identify the states they receive by means of standard homodyne detection measurements

photons during propagation of the key distributing state, given by Eq. 2. The most general expression of interest for investigating it is that of the time evolution of the corresponding state of the two-mode system. For the purpose of illustration of the effect of this noise on coherent states, let us first review a simple case, one in which entangled quantum states are prepared in an extreme case where $|\alpha_+\rangle = |\alpha\rangle$, $|\alpha_-\rangle = |-\alpha\rangle$, $|\beta_-\rangle = |-\alpha\rangle$, and $|\beta_+\rangle = |\alpha\rangle$, that is, one begins with the entangled coherent state considered in [6], namely

$$|\Psi\rangle = N_\alpha^{\pm}\left(|\alpha\rangle|-\alpha\rangle \pm |-\alpha\rangle|\alpha\rangle\right), \tag{3}$$

where $N_\alpha^{\pm} = 1/\sqrt{2 \pm 2\mathrm{e}^{-4|\alpha|^2}}$. This is a state of the form of Eq. 2 where $\alpha_+ = \beta_+ = \alpha, \alpha_- = \beta_- = -\alpha, \phi = \frac{\pi}{2}$, and $\theta = 0, \pi$. The effect on the outer product of two coherent states, under the standard assumption that the number of photons in the environment of the transmitted states is very small within the optical frequency range of the states involved, can be written

$$|\alpha\rangle\langle\beta| \to \exp\left[-(1-\kappa)\left\{\left(|\alpha|^2 + |\beta|^2\right)/2 - \alpha\beta^*\right\}\right]|\sqrt{\kappa}\alpha\rangle\langle\sqrt{\kappa}\beta|, \tag{4}$$

where $\kappa \equiv \mathrm{e}^{-\gamma\tau}$, with γ being the decay constant for the medium, so that the resulting density matrix for the state is

$$\rho_\pm(\tau) = (N_\alpha^{\pm})^2\left\{|t\alpha\rangle\langle t\alpha| \otimes |-t\alpha\rangle\langle -t\alpha| + |-t\alpha\rangle\langle -t\alpha| \otimes |t\alpha\rangle\langle t\alpha| \pm \mathrm{e}^{4\alpha^2 r^2}\right.$$
$$\left.\times\ (|t\alpha\rangle\langle -t\alpha| \otimes |-t\alpha\rangle\langle t\alpha| + \mathrm{h.c.})\right\}, \tag{5}$$

where $t = \sqrt{\kappa}$ and $r = \sqrt{1-t^2}$ is a normalized time parameter, cf. e.g., [18,19]. The most useful representation of states $\rho_\pm(\tau)$ is that in the basis

$$|\pm\rangle = \left(N_\alpha^{\pm}\right)\left(|t\alpha\rangle \pm |-t\alpha\rangle\right). \tag{6}$$

Our interest here is in antisymmetric states of the type $\rho_-(\tau)$, which in this basis has taken the form

$$\rho_\pm(\tau) = \left(N_\alpha^\pm/\sqrt{2}\right)^2 \begin{pmatrix} A & 0 & 0 & D \\ 0 & B & -B & 0 \\ 0 & -B & B & 0 \\ D & 0 & 0 & C \end{pmatrix}, \tag{7}$$

where

$$A = \mathrm{e}^{4(1-r^2)\alpha^2}\left(-1+\mathrm{e}^{4r^2\alpha^2}\right)\left(1+\mathrm{e}^{-2(1-r^2)\alpha^2}\right)^2 \tag{8}$$

$$B = -1+\mathrm{e}^{4\alpha^2}-\mathrm{e}^{4r^2\alpha^2}+\mathrm{e}^{4(1-r^2)\alpha^2} \tag{9}$$

$$C = \mathrm{e}^{4(1-r^2)\alpha^2}\left(-1+\mathrm{e}^{4r^2\alpha^2}\right)\left(-1+\mathrm{e}^{2(1-r^2)\alpha^2}\right)^2 \tag{10}$$

$$D = -1-\mathrm{e}^{4\alpha^2}+\mathrm{e}^{4r^2\alpha^2}+\mathrm{e}^{4(1-r^2)\alpha^2}, \tag{11}$$

of a form often called X-state form [20].

In the more realistic case where the entangling mechanism using Kerr nonlinearities is unable to create states of the form of Eq. 3 due to the difficulty of obtaining large phase shifts, the density matrix is of a less simple form. However, the effect of photon loss noise on the QKD signal states in such cases, which remain of the form of Eq. 2 with smaller induced phase shifts $-\phi$, can be considered effectively via corresponding annihilation operators, namely

$$\hat{a}_j \to t_j\hat{a}_j + \sqrt{1-t_j^2}\,\hat{a}_j^{(E)} \tag{12}$$

where E denotes the vacuum or environment and j labels orthogonal states. This approach suffices to provide us with the necessary information for practically analyzing the effects of noise and eavesdropping. In particular, this can be done by directly considering the effects of the noise on beam correlations, as demonstrated in the following section. Because an eavesdropper, Eve, may readily obtain a portion of the signal beam transmitted by Alice and infer its state, she would be capable of determining the key if her activity were to go undetected. Thus, one needs a means for detecting her activity. Once any effect on states consistent with eavesdropping is discovered, one can remove from the transmitted key any key bit values which may have been so discovered.

4 Eavesdropper detection

The method for detecting eavesdropping using entanglement witnessing naturally fits our entangled coherent signal states. An *entanglement witness* $\mathcal{S}$ is defined as a quantity such that $\mathcal{S} < 0$ whenever a system is entangled. When $\mathcal{S} \geq 0$, in general, the entanglement or separability of the system cannot be inferred from such a quantity. Nonetheless, so-called *strong entanglement witnesses* also exist, which provide

both necessary *and* sufficient conditions for entanglement. In particular, for entangled Gaussian states of the electromagnetic field, which include the coherent states, there is a witness [21] based on the positive partial trace criterion [16,22] which can be made use of here.

Before looking at a true entanglement witness for the system in question, let us first look at a different quantity $\mathcal{W}$, which in Ref. [4] we referred to as an *eavesdropping witness*. To understand this quantity, let us assume that $\hat{q}_1$, $\hat{p}_1$ is pair of orthogonal quadratures for beam A and $\hat{q}_2$, $\hat{p}_2$ is the corresponding pair of quadratures for B. Then one can form the vector $\hat{\xi} = \left(\hat{q}_1, \hat{p}_1, \hat{q}_2, \hat{p}_2\right)$ and the *covariance matrix*, defined as the 4×4 matrix, with elements $V_{ij} = \frac{1}{2}\langle\left\{\hat{\xi}_i - \langle\xi_i\rangle, \hat{\xi}_j - \langle\xi_j\rangle\right\}\rangle$, where $\{.. , .. \}$ denotes the anticommutator and angular brackets denote expectation value. V itself is expressed in terms of three 2×2 matrices as $V = \begin{pmatrix} A_1 & C \\ C^T & A_2 \end{pmatrix}$; A_1 and A_2 are the self-covariance matrices of each of beam separately, while C describes correlations between the two. One pertinent entanglement witness ([21]) derived from the covariance matrix is

$$\mathcal{W} = 1 + \det V + 2\det C - \det A_1 - \det A_2. \tag{13}$$

For coherent states, the system is entangled if and only if $\mathcal{W} < 0$. It is particular helpful that V is experimentally measurable. In order to find V, Alice and Bob can make quadrature measurements and compare their results. The covariance submatrices are affected by noise, which has the effect of the transformation of annihilation operators shown in Eq. 12, as follows.

$$C \to C' = t_1 t_2 C, \tag{14}$$

$$A_j \to A'_j = t_j^2\left(A_j - \frac{1}{4}I\right) + \frac{1}{4}I, \tag{15}$$

where I is the corresponding identity matrix.

The quantity $\mathcal{W}$ is a strong entanglement witness for Gaussian systems [17,21]. For reasons described in [4], $\mathcal{W}$ is not a true entanglement witness for the entangled coherent state system of Sect. 2. However, it does cross from negative to positive values with distance, similar to the case of an entanglement witness in the presence of ESD, and it does so at a distance that strongly correlates with a sudden change in the value of the true entanglement witness $\mathcal{S}$ defined below [4]. This distance decreases in the presence of eavesdropping; $\mathcal{W}$ is thus in some sensitive to changes in the entanglement of the system and provides a practical useable signal of eavesdropping.

In the case we are considering, the coherent states are not orthogonal as the pairs $\{|\alpha\rangle, |-\alpha\rangle\}$ and $\{|\beta\rangle, |-\beta\rangle\}$ themselves were in the previous section. Nonetheless, many of the expressions for these states differ from those obtained in the ideal case by exponentially small terms only: These terms are negligible for beams of sufficient amplitude such as we consider here. In propagation of the signal, the transmission matrices take form $t_j = \mathrm{e}^{-\frac{1}{2}K_j d_j}$, where d_j is the propagation distance in each arm. One then uses these to determine the distances over which $\mathcal{W}$ changes sign. The effect on coherence states in two configurations of state source with Alice or state source

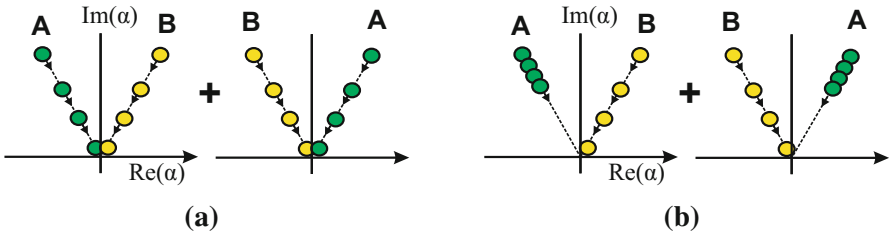

Fig. 3 (Color online) **a** Symmetric decay: entanglement decays more rapidly due to state overlap. **b** Asymmetric decay: entanglement decays more slowly because overlap occurs less quickly. The entanglement decay rate controlled by the most slowly decaying state

midway between Alice and Bob, the symmetric and the asymmetric, is illustrated in Fig. 3a, b, respectively.

In particular, indicating loss rates in the two arms of the QKD system we are considering by K_1 and K_2, one finds

$$V = \begin{pmatrix} A_1' & C' \\ C'^{T} & A_2' \end{pmatrix} = \begin{pmatrix} a_1' & 0 & b' & 0 \\ 0 & a_1' & 0 & c' \\ b' & 0 & a_2' & 0 \\ 0 & c' & 0 & a_2' \end{pmatrix}, \tag{16}$$

$$a_j'(d_1, d_2) = \left(a - \frac{1}{4}\right) \mathrm{e}^{-K_j d_j} + \frac{1}{4} \tag{17}$$

$$b'(d_1, d_2) = b\ \mathrm{e}^{-\frac{1}{2}(K_1 d_1 + K_2 d_2)} \tag{18}$$

$$c'(d_1, d_2) = c\ \mathrm{e}^{-\frac{1}{2}(K_1 d_1 + K_2 d_2)}, \tag{19}$$

where $j = i, 2, a, b$, and c are the values of a', b', and c' at before propagation, which are:

$$a = \frac{|\alpha N|^2}{2} f(\theta, \phi) - \frac{1}{2}|\alpha|^2 + \frac{1}{4} \tag{20}$$

$$b = \frac{|\alpha N|^2}{2} g(\theta, \phi) - \frac{1}{2}|\alpha|^2 \cos 2\phi \tag{21}$$

$$c = \frac{|\alpha N|^2}{2} g(\theta, \phi) - \frac{1}{2}|\alpha|^2, \tag{22}$$

where $f(\theta, \phi) = \left[1 + \cos 2\phi \cos\theta \mathrm{e}^{-4|\alpha|^2 \sin^2\phi}\right]$ and $g(\theta, \phi) = [\cos 2\phi + \cos\theta \mathrm{e}^{-4|\alpha|^2 \sin^2\phi}]$. These results hold for $|\alpha\phi| >> 1$; for the exact expressions, see [4]. Note that the normalization N also implicitly depends on the two propagation distances d_j.

When the QKD system is configured so that the initial signal state $|\phi\rangle$ is produced in the laboratory of Alice, $d_1 \approx 0$, so that:

$$\mathcal{W} = 1 + b^2c^2\mathrm{e}^{-2K_2d_2} + a^2\left(\left(a-\frac{1}{4}\right)\mathrm{e}^{-K_2d_2}+\frac{1}{4}\right)^2 - (b^2+c^2)\,\mathrm{e}^{-K_2d_2}\,a\left(\left(a-\frac{1}{4}\right)\mathrm{e}^{-K_2d_2}+\frac{1}{4}\right) + 2bc\left(\mathrm{e}^{-K_2d_2}\right) - a^2 - \left(\left(a-\frac{1}{4}\right)\mathrm{e}^{-K_2d_2}+\frac{1}{4}\right)^2. \tag{23}$$

As shown in Fig. 4, $\mathcal{W}$ starts with large negative values when the second configuration leg is a zero distance, $d_2 = 0$. It then falls off dramatically with distance due to the photon loss of the type described above. $\mathcal{W}$ decays toward zero and then changes sign at a finite distance, which can be seen by careful examination of Fig. 5: This crossing by $\mathcal{W}$ of the d-axis is analogous to the signaling of entanglement death at finite distance (ESD) [23–25].

This exponential decay of the above terms is guided by the decrease in the magnitude $|\alpha|$ and thus in average photon number. When ϕ is small enough to make the approximation $\sin\phi \approx \phi$ valid, one already finds $\mathrm{e}^{-4|\alpha|^2\sin^2\phi} \approx \mathrm{e}^{-4(|\alpha|\phi)^2}$ falling to the value .01 for $|\alpha\phi| > 1.08$; the terms involving the exponentials can therefore be neglected when $|\alpha\phi|$ is much greater than 1. In that range, one has the simple forms for the parameters $a = \frac{1}{4}$ and $b = 0, c = -|\alpha|^2\sin^2\phi$ of the general forms given by Eqs. (20)–(22), allowing for concise expressions for the distance at which a sign change occurs. In particular, one has in the symmetrical configuration where the distances to Alice and Bob from the signal source are the same and assuming that the loss parameter K is equal, so that when $K_1d_1 = K_2d_2 \equiv Kd$, without restricting ϕ, one finds that $\mathcal{W}$ changes sign when $|\alpha(d)| = \sqrt{\frac{15}{4}}\ \csc\phi$, so that there is crossing of the axis at $d = \frac{2}{K}\ln\left(\sqrt{\frac{4}{15}}\alpha\sin\phi\right)$. For the asymmetrical configuration in which Alice produces signal states in her laboratory, crossing occurs at $d_2 = \frac{4}{K}\ln\left(\sqrt{\frac{4}{15}}\alpha\sin\phi\right)$.

In this asymmetric configuration, the state $|\psi(d_1, d_2)\rangle$ at distances d_1 and d_2 along the two branches is given by Eq. 2 with $\alpha_\pm \to \alpha_\pm\mathrm{e}^{-\frac{1}{2}K_1d_1}$, $\beta_\pm \to \beta_\pm\mathrm{e}^{-\frac{1}{2}K_2d_2}$, so that

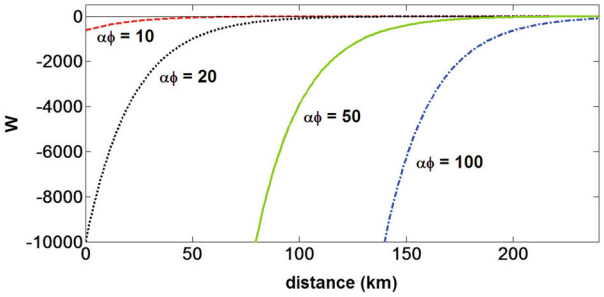

Fig. 4 (Color online) Eavesdropping witness versus distance under the photon loss mechanism, assuming no loss on Alice's side. The parameter values are: $\alpha = 1000, \phi = .01$ (*red dashed*), $\alpha = 2000, \phi = .01$ (*black*, *dotted*), $\alpha = 1000, \phi = .05$ (*green solid*), $\alpha = 1000, \phi = .1$ (*blue dash-dot*). The value $K = .046\ \mathrm{km}^{-1}$ is used for the 1550 nm telecom window

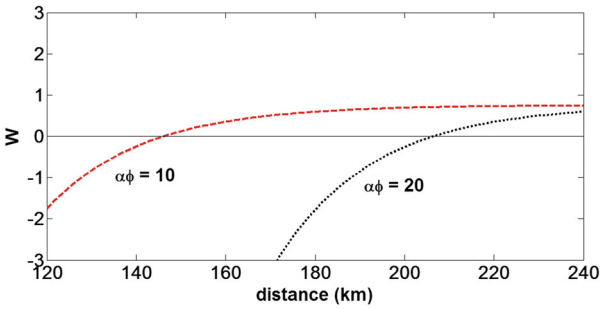

Fig. 5 (Color online) A portion of the previous figure magnified to show the portion where $\mathcal{W}$ curves cross the d-axis. In the absence of eavesdropping, the crossing point is determined by the initial amplitude of the coherent states

$$|\psi\rangle = \frac{N}{2}\left[|\alpha_+ e^{-\frac{1}{2}K_1 d_1}\rangle|\alpha_- e^{-\frac{1}{2}K_2 d_2}\rangle + e^{i\theta}|\alpha_- e^{-\frac{1}{2}K_1 d_1}\rangle|\alpha_+ e^{-\frac{1}{2}K_2 d_2}\rangle\right]. \quad (24)$$

The overlap between states of this entangled superposition state increases as they both decay in average photon number toward the same state of zero photons, as shown in Fig. 3a. When the losses along the two arms differ, the states can be seen to move away from each other in phase space, as shown in Fig. 3b, causing the crossing distance to increase. This occurs for example in the most extreme asymmetric case, where there is no loss in Alice's arm, but Bob's state decays toward the origin. Even in this extreme case, entanglement will still eventually be lost, since for large d_2 the state becomes

$$|\psi(0, d_2)\rangle \approx \frac{N}{2}\left(|\alpha e^{i\phi}\rangle_A + e^{i\theta}|\alpha e^{-i\phi}\rangle_A\right) \times |vac\rangle_B, \quad (25)$$

which is of product form and, so, unentangled.

If the eavesdropper, Eve, attempts to learn the signal state, she will change the detected value of the two quadratures, whose measurement is part of the overall QKD system design shown schematically in Fig. 2. Suppose an unauthorized experimenter makes measurements of either or both quadratures of $\hat{q}$ and $\hat{p}$, the amplitude and phase quadratures, respectively. The measurement of one quadrature will cause an increase in the conjugate quadrature, leading to an increase in the overlap of the two coherent states in phase space and a consequent drop in entanglement. The effect is similar to that of photon loss: The photon loss can be modeled as the insertion of a beam splitter in the beam, leading to increased noise from vacuum fluctuations in the unused port. This vacuum noise similarly causes the quadratures to increase. The result is that eavesdropping causes the system to act as if it has propagated a larger distance than it actually has, and the effect of this can be seen by measuring $\mathcal{W}$.

The effect of eavesdropping on the eavesdropping witness $\mathcal{W}$ is shown in Fig. 6 for a set of different degrees of eavesdropping strength, assuming that all gains are unity and that detector noise may be neglected. One notes in particular that as eavesdropping strength increases, as parameterized by the fraction $|r|^2$ of beam intensity taken out of the beam be Eve's extraction beam splitter, $\mathcal{W}$ is affected in the same manner as by

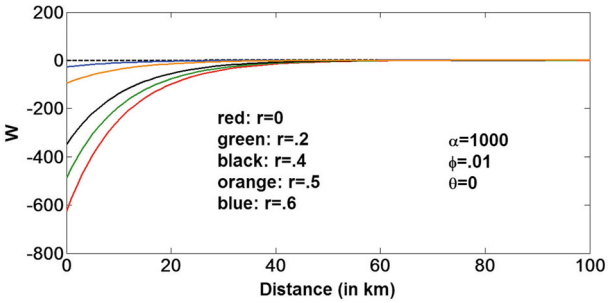

Fig. 6 (Color online) As the strength of eavesdropping attack (as parameterized by $|r|^2$) increases, the $\mathcal{W}$ curves decay faster and the location of the crossing point where $\mathcal{W}$ changes sign appear at smaller distances, thus signaling eavesdropping

transmission losses but prematurely, so that the distance at which crossing occurs is shortened.

One chief advantage of using $\mathcal{W}$ instead of a true entanglement witness is that $\mathcal{W}$ is easy to measure, requiring only standard homodyne techniques. However, we can also look at a true entanglement witness, such as the measure $\mathcal{S}$, first introduced in [30], and see whether true ESD occurs. $\mathcal{S}$ is defined by the determinant

$$\mathcal{S} = \begin{vmatrix} 1 & \langle \hat{b}^\dagger \rangle & \langle \hat{a}\hat{b}^\dagger \rangle \\ \langle \hat{b} \rangle & \langle \hat{b}^\dagger \hat{b} \rangle & \langle \hat{a}\hat{b}^\dagger \hat{b} \rangle \\ \langle \hat{a}^\dagger \hat{b} \rangle & \langle \hat{a}^\dagger \hat{b}^\dagger \hat{b} \rangle & \langle \hat{a}^\dagger \hat{a} \hat{b}^\dagger \hat{b} \rangle \end{vmatrix} . \tag{26}$$

Here $\hat{a}$ is the annihilation operator at Alice's location and $\hat{b}$ is the corresponding operator for Bob's. This witness is valid for any state, Gaussian, or otherwise. Alternatively, we could consider

$$\tilde{\mathcal{S}} = \begin{vmatrix} 1 & \langle \hat{a}^2 \rangle & \langle \hat{a}\hat{b}^\dagger \rangle \\ \langle \hat{a}^{\dagger 2} \rangle & \langle \hat{a}^{\dagger 2} \hat{a}^2 \rangle & \langle \hat{a}^{\dagger 2} \hat{a} \hat{b}^\dagger \rangle \\ \langle \hat{a}^\dagger \hat{b} \rangle & \langle \hat{a}^\dagger \hat{a}^2 \hat{b}^\dagger \rangle & \langle \hat{a}^\dagger \hat{a} \hat{b}^\dagger \hat{b} \rangle \end{vmatrix} . \tag{27}$$

Both $\mathcal{S}$ and $\tilde{\mathcal{S}}$ are capable of detecting entanglement in non-Gaussian system states, and each of them is capable of detecting some forms of entanglement that are missed by the other.

Here, we consider $\mathcal{S}$. For small displacement angle ϕ, $\mathcal{S}$ is negative definite (Fig. 7), indicating an asymptotic decay of entanglement. However, if ϕ grows larger, ESD can occur. For example, for $\phi = 1.5$ rad, we see (Fig. 7) that the witness goes from zero to a positive value at a finite distance, signaling ESD. Holding all other parameters fixed, the value of $\mathcal{S}$ reaches its maximum positive value at $\phi = \frac{\pi}{2}$, that is, when the states $|\alpha\pm\rangle$ are simply the orthogonal pair $|\pm\alpha\rangle$ and the entangled state is simply that of Eq. 3. Figure 8 shows the situation in the absence of eavesdropping. In the presence of even mild eavesdropping, $\mathcal{S}$ becomes positive immediately after the eavesdropping and then decays monotonically back to zero. So, once again, the alteration of the behavior of the witness with distance provides a clear signal of tampering.

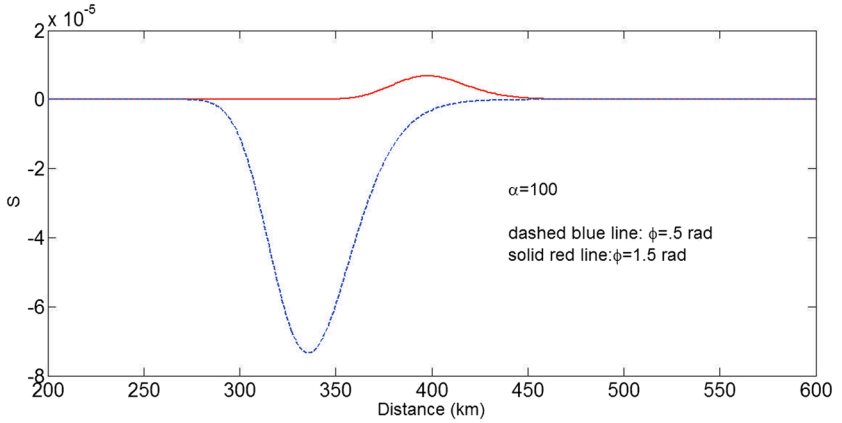

Fig. 7 (Color online) For small phase shifts, the entangled coherent states have values of entanglement witness $\mathcal{S}$ that are negative semi-definite (*dashed blue line*). However, for larger phase shifts, it is possible for $\mathcal{S}$ to become positive at finite distance (*solid red line*), indicating ESD

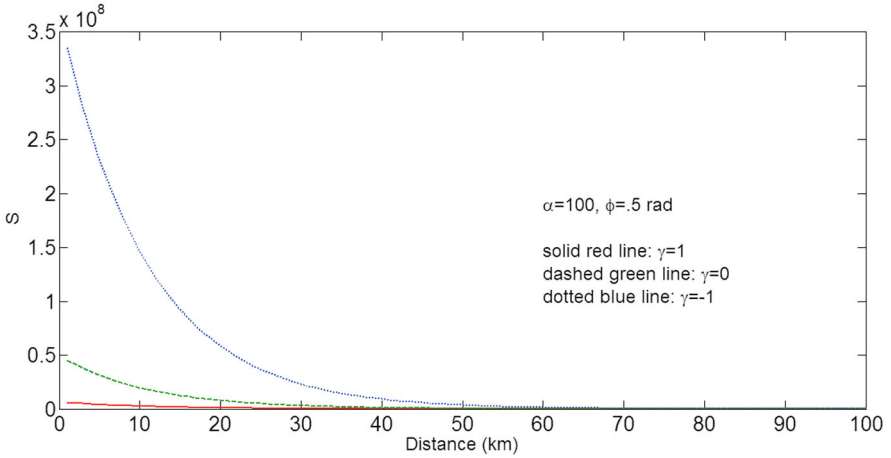

Fig. 8 (Color online) When eavesdropping is added, the behavior of $\mathcal{S}$ is dramatically different from that illustrated in the previous figure. Even a small amount of eavesdropping causes the value of $\mathcal{S}$ to become positive after the eavesdropping. It then decays monotonically to zero. Here, by contrast, it is assumed for simplicity that the eavesdropping occurs near the source. The three curves are for different values of γ, a parameter that characterizes the information gain of the eavesdropper: For $\gamma > 0$, Eve gains little information but also causes little disturbance, while for $\gamma < 0$ she gains more information at the expense of making her actions more visible. As Eve obtains more information, the entanglement witness reaches larger positive values

We see then that if appropriately chosen entangled states can be generated, then eavesdropper detection in a QKD system can be provided by ESD, allowing QKD to be securely conducted over long distances with strong beams.

5 Experimental measurement of witnesses

Unlike $\mathcal{W}$, both $\mathcal{S}$ and $\tilde{\mathcal{S}}$ involve moments that are of higher than quadratic order in the quadratures q and p, and so cannot be measured via simple homodyne detection. It is the presence of these higher-order moments that allow them to detect non-Gaussian types of entanglement that are missed by simpler witnesses. Here we briefly describe how these and other higher-order entanglement witnesses may be experimentally measured.

The system below (Figs. 9, 10) is capable of measuring both of these, or more generally, of measuring any entanglement witness formed by up to four creation or annihilation operators in each mode (a or b). It is a special case of the method described in [31] and [32] for the measurements of arbitrary normal-ordered moments of optical creation and annihilation operators. (Note that $\mathcal{S}$ and $\tilde{\mathcal{S}}$ are both normal ordered: The creation operators for each mode are to the left of their matching annihilation operators.) To measure $\mathcal{S}$, we need to be able to measure the actions of operators $\hat{a}$, $\hat{a}^\dagger$, and $\hat{a}^\dagger\hat{a}$ in Alice's laboratory and the corresponding operators $\hat{b}$, $\hat{b}^\dagger$, and $\hat{b}^\dagger\hat{b}$ in Bob's laboratory.

The actions of the beam splitters and phase shifts can be readily traced through the system to find the outputs at each detector. The result in Alice's laboratory is that the current at the jth detector is

$$\hat{I}_{A_j} = \hat{a}_j^\dagger \hat{a}_j, \tag{28}$$

for $j = 1, 2, 3, 4$, where:

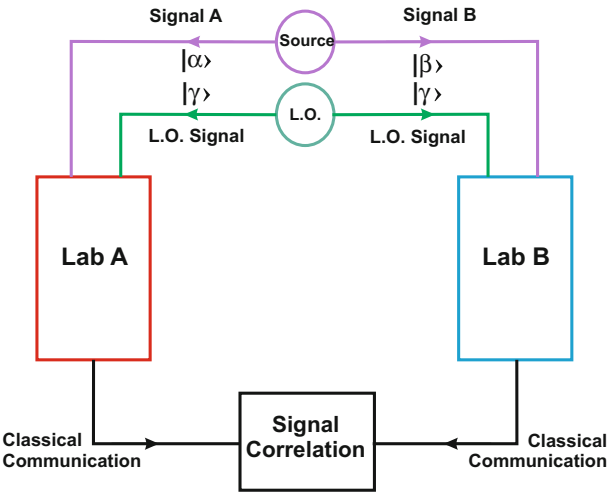

Fig. 9 The setup for measuring expectation values of arbitrary products of creation and annihilation operators up to fourth order at each of two locations (*Lab A* and *Lab B*). Along with the entangled signal, each laboratory is sent an identical local oscillator signal. Measurements of photocurrents are made in each laboratory (see below) and then correlated via the classical communication channel

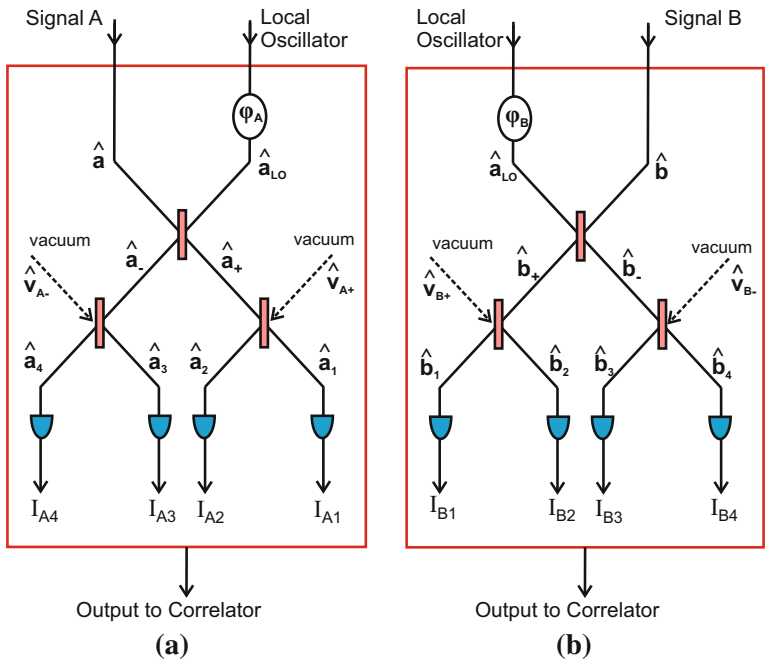

Fig. 10 **a** Interior of Alice's laboratory. Alice can control the phase shift ϕ_A. The light strikes four photodetectors at the *bottom*, producing four photocurrents, $I_{A1}, \ldots, I_{A4}$. All the necessary operator moments can be obtained from measuring the correlations between these four currents and four similar currents in Bob's laboratory. **b** Bob's laboratory is a mirror image of Alice's laboratory, with all A's replaced by B's

$$\hat{a}_1 = \frac{1}{2}\left(\hat{a} + i\hat{a}_{\mathrm{LO}}\right) + \frac{i}{\sqrt{2}}\hat{v}_{A+} \tag{29}$$

$$\hat{a}_2 = \frac{i}{2}\left(\hat{a} + i\hat{a}_{\mathrm{LO}}\right) + \frac{1}{\sqrt{2}}\hat{v}_{A+} \tag{30}$$

$$\hat{a}_3 = -\frac{1}{2}\left(\hat{a} - i\hat{a}_{\mathrm{LO}}\right) + \frac{1}{\sqrt{2}}\hat{v}_{A-} \tag{31}$$

$$\hat{a}_4 = \frac{i}{2}\left(\hat{a} - i\hat{a}_{\mathrm{LO}}\right) + \frac{i}{\sqrt{2}}\hat{v}_{A-}, \tag{32}$$

where $\hat{v}_{A\pm}$ represent the annihilation operators at the unused beam splitter ports. Because the operators we are examining are already normal-ordered, there are no commutators that can lead to these vacuum operators coming into play; therefore, the $\hat{v}_{A\pm}$ can be safely ignored.

Assume that the local oscillator (of amplitude γ) is strong enough to be treated classically. Then if we take the difference between two of the currents, we obtain the quadratures of the signal:

$$\hat{I}_{A_1} - \hat{I}_{A_3} = \hat{I}_{A_2} - \hat{I}_{A_4} \tag{33}$$

$$= \frac{\gamma}{2}\left(\hat{a}^\dagger\, \mathrm{e}^{-i\psi_A} + \hat{a}\, \mathrm{e}^{+i\psi_A}\right) \tag{34}$$

$$= \gamma \hat{Q}_A(\psi_A), \tag{35}$$

where $\psi_A = \left(\phi_A + \frac{\pi}{2}\right), \phi_A$ is the phase shift given to the local oscillator in Alice's laboratory, and $\hat{Q}_A(\psi_A)$ is the quadrature at angle ψ_A. As special cases, $\hat{Q}_A(0) = \hat{q}_A = \frac{1}{2}\left(\hat{a} + \hat{a}^\dagger\right)$ and $\hat{Q}_A(-\frac{\pi}{2}) = \hat{p}_A = \frac{i}{2}\left(\hat{a}^\dagger - \hat{a}\right)$ are the "position" and "momentum" quadratures of the signal. So measuring the expectation value of the difference $\langle \hat{I}_{A_1} - \hat{I}_{A_2} \rangle$ at two phase shifts allows us to find $\langle \hat{q}_A \rangle$ and $\langle \hat{p}_A \rangle$; then taking the sum and difference of these gives us $\langle \hat{a} \rangle$ and $\langle \hat{a}^\dagger \rangle$.

Taking the sum of the two phase shifts instead of the difference, we obtain

$$\hat{I}_{A_1} + \hat{I}_{A_3} = \hat{I}_{A_2} + \hat{I}_{A_4} \tag{36}$$

$$= \frac{1}{2}\left(\hat{a}^\dagger \hat{a} + |\gamma|^2\right), \tag{37}$$

so the known local oscillator amplitude γ can be subtracted off to get $\langle \hat{a}^\dagger \hat{a} \rangle$ from $\langle \hat{I}_{A_1} + \hat{I}_{A_2} \rangle$:

$$\langle \hat{a}^\dagger \hat{a} \rangle = 2\langle \hat{I}_{A_1} + \hat{I}_{A_2} \rangle - |\gamma^2|. \tag{38}$$

The expectation operators on Bob's side are obtained in a similar manner. Finally, multiplying signals from Alice's and Bob's laboratory allows the building up of expectation values such as

$$\langle \hat{a}^\dagger \hat{b}^\dagger \hat{b} \rangle = \left\langle \left[\left(\hat{I}_{A_1}(0) - \hat{I}_{A_2}(0) \right) + i \left(\hat{I}_{A_1}\left(-\frac{\pi}{2}\right) - \hat{I}_{A_2}\left(-\frac{\pi}{2}\right) \right) \cdot \left(2\left(\hat{I}_{B_1} + \hat{I}_{B_2} \right) - |\gamma|^2 \right) \right] \right\rangle \tag{39}$$

and

$$\langle \hat{a}^\dagger \hat{a} \hat{b}^\dagger \hat{b} \rangle = \left\langle \left(2\left(\hat{I}_{A_1} + \hat{I}_{A_2} \right) - |\gamma|^2 \right) \cdot \left(2\left(\hat{I}_{B_1} + \hat{I}_{B_2} \right) - |\gamma|^2 \right) \right\rangle. \tag{40}$$

So we can build all of the entries of $\mathcal{S}$ from correlations between sums and differences of easily measurable photocurrents.

In a similar manner, all of the moments needed for the other entanglement witness $\tilde{\mathcal{S}}$ can also be derived from the same arrangement. Notice that for $\mathcal{S}$, we really only need two of the four detectors in each laboratory. For $\tilde{\mathcal{S}}$ or for other witnesses, all four of the detectors in each laboratory will be needed, in order to build up expectation values of the form $\langle \hat{a}^2 \rangle$, $\langle \hat{a}^{\dagger 2} \hat{a}^2 \rangle$, $\langle \hat{a}^{\dagger 2} \hat{a} \hat{b}^\dagger \rangle$, etc.

6 Conclusions

The design and principles of operation of a coherent state-based quantum key distribution system based on the occurrence of entanglement sudden death and its early onset due to the intervention of any eavesdropper were presented. This involved the explanation of the effects of photon loss during signal state transmission and similar but additional effect of eavesdropping leading to premature ESD. This system is noteworthy because of its use of an entanglement witness for the eavesdropping detection and advantage of the system over traditional fixed, few photon number signal-based

QKD system in that it can operate with the ability to avoid key string detection by eavesdroppers, as shown here, over distances of the order of one hundred kilometers. Specific methods for measuring the witness used by the QKD method have been provided as well as a detailed explanation of the anticipated behavior of them under expected eavesdropping conditions.

Acknowledgments This research was supported by the DARPA QUINESS program through US Army Research Office award W31P4Q-12-1-0015.

References

1. Ekert, A.K.: Quantum cryptography based on Bell's theorem. Phys. Rev. Lett. **67**, 661 (1991)
2. Jaeger, G., Sergienko, A.V.: Entanglement sudden death: a threat to advanced quantum key distribution? Nat. Comput. **13**, 459 (2014)
3. Jaeger, G., Simon, D., Sergienko, A.V.: Implications of disentanglement and locality induction for quantum information processing and cryptography. Quantum Matter **2**, 427 (2013)
4. Simon, D.S., Jaeger, G., Sergienko, A.V.: Coherent state quantum key distribution with entanglement witnessing. Phys. Rev. A **89**, 012315 (2014)
5. Sanders, B.C.: Entangled coherent states. Phys. Rev. A **45**, 6811 (1992)
6. Rice, D.A., Jaeger, G., Sanders, B.C.: Two-coherent-state interferometry. Phys. Rev. A **62**, 012101 (2000)
7. Boeuf, N., Branning, D., Chaperot, I., Dauler, E., Guerin, S., Jaeger, G., Muller, A., Migdall, A.L.: Calculating characteristics of noncollinear phase matching in uniaxial and biaxial crystals. Opt. Eng. **9**, 1016–1024 (2000)
8. Kirby, B.T., Franson, J.D.: Nonlocal interferometry using macroscopic coherent states and weak nonlinearities. Phys. Rev. A **87**, 053822 (2013)
9. Simon, D.S., Jaeger, G., Sergienko, A.V.: Quantum information in communication and imaging. Int. J. Quantum Inf. **12**, 1430004 (2014)
10. Nemoto, K., Munro, W.J.: Nearly deterministic linear optical controlled-NOT gate. Phys. Rev. Lett. **93**, 250502 (2004)
11. Munro, W.J., Nemoto, K., Spiller, T.P.: Weak non-linearities: a new route to optical quantum computation. New J. Phys. **7**, 137 (2005)
12. Lukin, M.D., Imamoglu, A.: Nonlinear optics and quantum entanglement of ultraslow single photons. Phys. Rev. Lett. **84**, 1419 (2000)
13. Harris, S.E., Field, J.E., Imamoglu, A.: Nonlinear optical processes using electromagnetically induced transparency. Phys. Rev. Lett. **64**, 1107 (1990)
14. Schmidt, H., Imamoglu, A.: Giant Kerr nonlinearities obtained by electromagnetically induced transparency Opt. Lett. **21**, 1936–1938 (1996)
15. Turchette, Q.A., Hood, C.J., Lange, W., Mabuchi, H., Kimble, H.J.: Measurement of conditional phase shifts for quantum logic. Phys. Rev. A **75**, 4710 (1995)
16. Horodecki, M., Horodecki, P., Horodecki, R.: Separability of mixed states: necessary and sufficient conditions. Phys. Lett. A **223**, 1–8 (1996)
17. Duan, L.-M., Giedke, G., Cirac, J.I., Zoller, P.: Inseparability criterion for continuous variable systems. Phys. Rev. Lett. **84**, 2722 (2000)
18. Park, K., Jeong, H.: Entangled coherent states versus entangled photon pairs for practical quantum-information processing. Phys. Rev. A **82**, 062325 (2010)
19. Phoenix, S.J.D.: Wave-packet evolution in the damped oscillator. Phys. Rev. A **41**, 5132 (1990)
20. Yu, T., Eberly, J.H.: Sudden death of entanglement: classical noise effects. Opt. Commun. **264**, 393–397 (2006)
21. Barbosa, F.A.S., de Faria, A.J., Coehlo, A.S., Cassemiro, K.N., Villar, A.S., Nussenzveig, P., Martinelli, M.: Disentanglement in bipartite continuous-variable systems. Phys. Rev. A **84**, 052330 (2011)
22. Peres, A.: Separability criterion for density matrices. Phys. Rev. Lett. **77**, 1413 (1996)
23. Yu, T., Eberly, J.H.: Sudden death of entanglement. Science **323**, 598–601 (2009)
24. Almeida, M.P., de Melo, F., Hor-Meyll, M., Salles, A., Walborn, S.P., Souto Ribeiro, P.H., Davidovich, L.: Environment-induced sudden death of entanglement. Science **316**, 579–582 (2007)

25. Ann, K., Jaeger, G.: Finite-time destruction of entanglement and non-locality by environmental influences. Found. Phys. **39**, 790 (2009)
26. Jaeger, G., Shimony, A., Vaidman, L.: Two interferometric complementarities. Phys. Rev. A **51**, 54 (1995)
27. Jaeger, G., Horne, M.A., Shimony, A.: Complementarity of one-particle and two-particle interference. Phys. Rev. A **48**, 1023 (1993)
28. Arthurs, E., Goodman, M.S.: Quantum correlations: a generalized Heisenberg uncertainty relation. Phys. Rev. Lett. **60**, 2447 (1988)
29. Paris, M.G.A.: The modern tools of quantum mechanics: a tutorial on quantum states, measurements, and operations. Eur. Phys. J. Special Topics **203**, 61–86 (2012)
30. Shchukin, E., Vogel, W.: Inseparability criteria for continuous bipartite quantum states. Phys. Rev. Lett. **95**, 230502 (2005)
31. Shchukin, E., Vogel, W.: Erratum: inseparability criteria for continuous bipartite quantum states. Phys. Rev. Lett. **96**, 200403 (2006)
32. Vogel, W., Shchukin, E.: Nonclassicality and entanglement: observable conditions. J. Phys. Conf. Ser. **84**, 012020 (2007)