Entangled-coherent-state quantum key distribution with entanglement witnessing

David S. Simon,[1,2] Gregg Jaeger,[2,3] and Alexander V. Sergienko[2,4,5]

[1]*Department of Physics and Astronomy, Stonehill College, 320 Washington Street, Easton, Massachusetts 02357, USA*

[2]*Department of Electrical and Computer Engineering, Boston University, 8 Saint Mary's Street, Boston, Massachusetts 02215, USA*

[3]*Division of Natural Sciences and Mathematics, Boston University, Boston, Massachusetts 02215, USA*

[4]*Photonics Center, Boston University, 8 Saint Mary's Street, Boston, Massachusetts 02215, USA*

[5]*Department of Physics, Boston University, 590 Commonwealth Avenue, Boston, Massachusetts 02215, USA*

(Received 23 May 2013; revised manuscript received 15 September 2013; published 15 January 2014)

An entanglement-witness approach to quantum coherent-state key distribution and a system for its practical implementation are described. In this approach, eavesdropping can be detected by a change in sign of either of two witness functions: an entanglement witness $\mathcal{S}$ or an eavesdropping witness $\mathcal{W}$. The effects of loss and eavesdropping on system operation are evaluated as a function of distance. Although the eavesdropping witness $\mathcal{W}$ does not directly witness entanglement for the system, its behavior remains related to that of the true entanglement witness $\mathcal{S}$. Furthermore, $\mathcal{W}$ is easier to implement experimentally than $\mathcal{S}$. $\mathcal{W}$ crosses the axis at a finite distance, in a manner reminiscent of entanglement sudden death. The distance at which this occurs changes measurably when an eavesdropper is present. The distance dependence of the two witnesses due to amplitude reduction and due to increased variance resulting from both ordinary propagation losses and possible eavesdropping activity is provided. Finally, the information content and secure key rate of a continuous variable protocol using this witness approach are given.

DOI: 10.1103/PhysRevA.89.012315 PACS number(s): 03.67.Dd, 03.65.Ud, 03.67.Hk, 42.50.Ex

I. INTRODUCTION

The goal of quantum key distribution (QKD) is for two participants (Alice and Bob) to generate a shared cryptographic key of bits in such a way that quantum mechanics prevents an eavesdropper (Eve) from obtaining significant information about the key without being detected. QKD schemes [1,2] based on the transmission of single photons or entangled photon pairs tend to be highly secure [3]. However, because single photons can be easily absorbed or deflected, the operational distances and key generation rates of these schemes are limited. It is often desirable to instead use pairs of entangled coherent states because individual-photon-level losses have little effect on them. Along with this benefit comes the challenge of revealing the action of eavesdroppers: it suffices for Eve to obtain only a small fraction of the coherent-state beam to measure the transmitted state. Moreover, although pairs of entangled coherent states can be created [4,5], randomly modulating them as needed for QKD is a nontrivial task.

Recently [6], a technique applicable to the detection of an eavesdropper on a quantum optical communication channel was proposed which involved phase entangling two coherent-state beams by interaction with a single photon inside a nonlinear medium. In that scheme, a beam splitter first puts a photon into a superposition of two possible path states. A phase shift is induced conditionally, depending on the path state, so that the pair of beams becomes phase entangled. Alice and Bob each receive one beam and make homodyne measurements to determine its phase. The relative phase between the beams determines the bit value to be used in the key. Effects due to eavesdropping are made detectable by introducing additional interferometers with controllable phase shifts σ_1 and σ_2 just before each of the detectors, respectively. Interference terms then appear in the joint detection rate as σ_1 and σ_2 are varied. If the beams have not been disturbed in transit, the visibility of this interference should be greater than $\frac{1}{\sqrt{2}} \approx 70.7\%$, suggesting stronger-than-classical correlations and violation of a Bell-type inequality. If the visibility drops below 70.7%, this could indicate that the beam has been tampered with. This method, in principle, allows phase-entangled states to be robustly distributed over large distances.

In this paper, we propose a technique for revealing eavesdroppers in systems for quantum key-bit distribution. This technique introduces entanglement in a manner similar to [6], but uses a fundamentally different approach to eavesdropper detection. Rather than using Bell violation for checking security, the idea is to instead look for degradation or death of entanglement due to Eve's actions by using functions designed to witness it [7,8]. The switch from measurements of nonlocal interference associated with a Bell-type inequality to direct entanglement-related witnesses provides substantial benefits: it both expands the effective operating distance and simplifies the required apparatus. The increase in operating distance is due to the fact that Bell violation is a stronger condition than entanglement. The particular entanglement witness $\mathcal{S}$ [9] used is negative for all finite distances when the coherent states propagate undisturbed; however, $\mathcal{S}$ changes sign to a positive value in the presence of eavesdropping, thus revealing Eve's intervention. Another related witness function $\mathcal{W}$, which is more easily measured but does not directly indicate entanglement in our system, can also serve this purpose.

As in [6], which involves the Bell inequality, the main goal of these functions is simply to reveal the presence of eavesdropping on the line; when the eavesdropper's signature is observed, the communicating parties know to shut down the line and seek another communication channel. The actual bits either may be derived from the entangled phases or they may arise from normal telecom approaches of modulating the intense coherent states. In this sense, the goal is to provide a "quantum tripwire" for practical use, as opposed to absolute

security in the sense that the phrase is commonly used in QKD. In other words, the basic idea is to take a more pragmatic approach to communication by providing an extra quantum-based layer of security to support highly efficient classical communication. As a result, our primary goal is less general and less difficult to achieve than other continuous variable protocols [10–16] that have been proposed with the goal of unconditional security in mind. Nonetheless, as discussed in Sec. VII, the witness approach is used directly on the key-bit transmitting system to provide security to fully quantum communication as well.

It is because the witness $\mathcal{S}$ itself involves third-order correlation functions, which may be inconvenient to implement experimentally, that we also consider the second witness function $\mathcal{W}$. $\mathcal{W}$ is related by rescaling of the quadratures to a well-known entanglement witness $\mathcal{W}_s$ [17,18], but is not in the strict sense a true entanglement witness in the current context. Despite this, it gives eavesdropper-detection results that match well with those of $\mathcal{S}$ and has the additional advantage that it is built from the covariance matrix of the system, which is easily accessible experimentally. $\mathcal{W}$ starts from an initially negative value, but then crosses the axis to positive values at finite distance, both during free propagation and in the presence of eavesdropping. This is closely analogous to the phenomenon of entanglement sudden death (ESD) [19], in which entanglement is lost after propagating a finite distance. The crossing occurs at a distance that can be easily predicted when there is no eavesdropping present. When eavesdropping occurs, the curve of $\mathcal{W}$ versus distance shifts by a measurable amount; in particular, there is a clear alteration of the distance at which the sign changes, allowing for easy detection.

We will collectively refer to quantities which are measurably altered by predictable amounts in the presence of eavesdropping as eavesdropping witnesses; both the true entanglement witness $\mathcal{S}$ and the additional function $\mathcal{W}$ are examples of such functions. It is shown that the two give consistent results for the distance over which the entanglement becomes unusable for eavesdropper detection.

Throughout this paper, coherent-state quadratures will be defined in terms of creation and annihilation operators via the relations

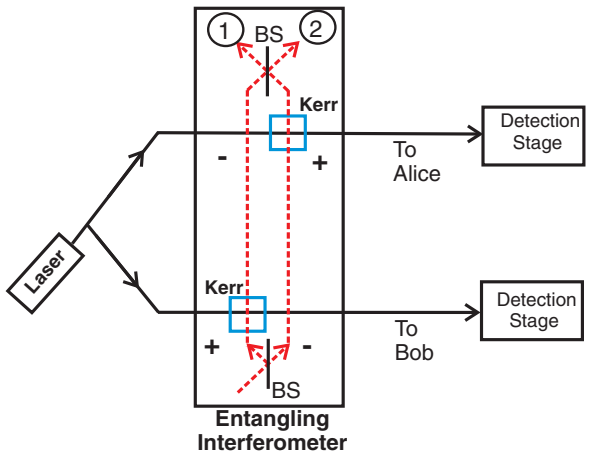
$$\hat{q} = \frac{1}{2}(\hat{a} + \hat{a}^\dagger), \quad \hat{p} = \frac{1}{2i}(\hat{a} - \hat{a}^\dagger). \tag{1}$$

It should be noted that there are several other normalization conventions that are common in the literature, with different constants in front on the right-hand side. Accordingly, when results from other authors are quoted in the following sections, the form used here may differ from their originally published forms by factors of two in some terms.

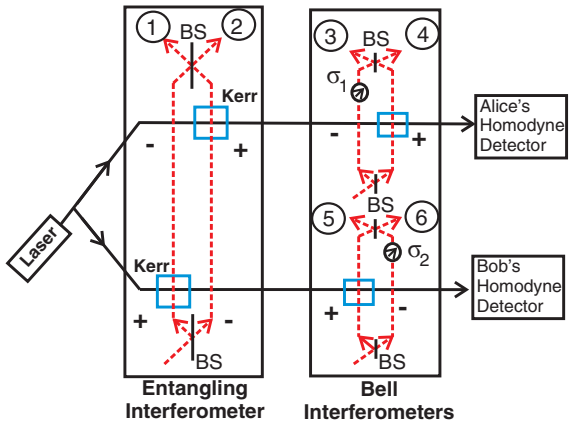
We begin in Sec. II by describing the entangled states under consideration and their means of production. The eavesdropping model assumed is described in Sec. III. There, we model the eavesdropping procedure by introducing a Gaussian cloner into the path of one of the coherent states. We then introduce the entanglement witness $\mathcal{S}$ and analyze its behavior in Sec. IV. In order to have a more convenient experimental measure, we then introduce $\mathcal{W}$ in Sec. V, and look in Sec. VI at some of its properties, with emphasis on its behavior under eavesdropping. A discussion of some information-related aspects in Sec. VII is then followed by a brief discussion of the results in Sec. VIII.

II. PHASE-ENTANGLED COHERENT STATES

The apparatus for the proposed system is shown in Fig. 1(a). A laser followed by a beam splitter produces a pair of optical coherent states, each in state $|\alpha\rangle$. As in [6], the coherent-state subsystem pair initially produced in state $|\alpha\rangle_A|\alpha\rangle_B$ becomes entangled in an interferometer by coupling to a single photon. A beam splitter first causes the photon state to enter a superposition of two path eigenstates. Then, if the photon is in the upper path state, beam B gains a phase shift 2ϕ due to cross-phase modulation of the photon with that beam in a



(a)



(b)

FIG. 1. (Color online) Schemes for phase-based coherent-state key distribution with single-photon triggers. (a) Scheme of the current paper. A beam splitter splits a laser beam into two beams in identical coherent states (solid black lines); a phase shifter compensates for the phase gained in the reflected state. A single photon also enters a superposition of two path states (dashed red lines). Due to the joint interaction of coherent state and the photon within Kerr media, the beams enter an equal-weight superposition of product states of pairs of oppositely phase-shifted coherent states. The specific form of the detection unit will be different for each of the applications to be discussed in the text. (b) Scheme of [6], with two additional interferometers to test for Bell violations.

nonlinear Kerr medium [20–25], whereas if the photon is in the lower path state, then there is a phase shift of 2ϕ in beam A. Finally, by adding another constant phase shift to each beam, we can arrange the output to be in the entangled state,

$$|\psi\rangle = \frac{N}{\sqrt{2}}(|\alpha_+\rangle_A|\alpha_-\rangle_B + e^{i\theta}|\alpha_-\rangle_A|\alpha_+\rangle_B), \tag{2}$$

where

$$|N|^{-2} = (1 + \cos\theta e^{-4|\alpha|^2\sin^2\phi}) \tag{3}$$

and $\alpha_\pm \equiv \alpha e^{\pm i\phi}$. (For simplicity, we do not explicitly indicate the single-photon states.) In the following, operators with subscripts 1 and 2, respectively, will correspond to Alice's beam and to Bob's beam.

Note that whereas $\pm\phi$ are the phase shifts of the coherent states within a given path state, θ is the relative phase between the two joint path states of the photon. The value of joint phase θ can be controlled by the experimenters: Keeping only events in which the photon is detected at detector 1 leads to $\theta = \pi$, while events in which it exits at detector 2 lead to $\theta = 0$. (Other values of θ can be achieved if desired by, for example, putting a piece of glass in one of the potential single-photon paths.) If the interferometer lacks stability, randomly varying phases in the single-photon paths could lead to decoherence. But these photons could be kept on a single bench in Alice's laboratory and be well controlled to prevent this. Fluctuations in the phases of the coherent states $|\alpha_\pm\rangle_A|\alpha_\mp\rangle_B \to |\alpha_\pm e^{i\delta\phi_1(t)}\rangle_A|\alpha_\mp e^{i\delta\phi_2(t)}\rangle_B$ would be a more serious problem because these are shared between laboratories that may be widely separated. This random phase variation is an independent source of entanglement loss, separate from the entanglement loss due to amplitude decay and eavesdropping. (We focus here on the latter, leaving the former to be discussed elsewhere.)

Using homodyne detection, each participant can measure the phase of his or her beam to determine the sign of its shift. Because the shifts in the two beams are always opposite, this is sufficient for Alice and Bob to obtain common key bits; for example, if Alice has $+\phi$ and Bob has $-\phi$, they can take the common bit value to be 0, while the opposite case then corresponds to 1.

Unfortunately, an eavesdropper may extract part of the beam and determine the bit transmitted. Although this cannot be *prevented*, it can be *detected*, so that Alice and Bob can prevent key material from being compromised by shutting down the communication line. Recall that for the purpose of revealing Eve's intervention, the proposal of [6] is to include two additional interferometers [Fig. 1(b)], each coupling one beam to another photon in order to detect nonlocal interference for Bell inequality tests. That approach has at least two limitations: (i) On the theoretical side, detecting Eve only requires *entanglement*, which in practice may still exist even when the Bell inequality is not violated [26]; thus, the setup tests for a less than ideal property. (ii) On the experimental side, simultaneous single-photon events are needed in *three independent interferometers*. This low-probability triple coincidence in widely separated interferometers is a significant practical limitation. The method given in the present paper avoids this problem by removing the need for more than one interferometer.

Because the amplitude of the input beam can be easily tuned, the system can be adjusted to work at different operating distances, potentially (as we see in the following sections) up to distances of several hundred kilometers. Current technology can realistically reach amplitudes $|\alpha|$ of up to 10^3–10^4 without doing damage to the fibers or producing high amounts of fluorescence and scattering; but for illustrative purposes of future potential, we have included plots with values of up to 10^6 at some points in the following.

III. THE EFFECT OF EAVESDROPPING

To examine measures against eavesdropping, we consider the case in which Eve attaches a Gaussian cloner [27] to one of the beams, which we assume to be Bob's. The cloner takes an input beam and makes two copies that have the same mean amplitude as the input. Eve keeps one beam and sends the other on to Bob. But, inevitably, there is a net increase in the variance of Bob's beam that will indicate her presence. Moreover, the more exact a copy Eve's beam is (i.e., the lower its variance), the larger the disturbance to Bob's beam. Specifically, if σ_{Bj} and σ_{Ej} (for $j = q, p$) are the added variances to Bob's beam and to Eve's beam, in excess of the initial variance, then these variance increases must satisfy [27]

$$\sigma_{Bq}^2\sigma_{Ep}^2 \geqslant \tfrac{1}{16},\ \ \sigma_{Bp}^2\sigma_{Eq}^2 \geqslant \tfrac{1}{16}. \tag{4}$$

For optimal cloning devices, the effect on the q and p quadratures should be the same; henceforth, we therefore assume that $\sigma_q^2 = \sigma_p^2 \equiv \sigma^2$ for all participants.

In addition to the increased variance, any cloning device will involve additional input ports besides the one carrying the state to be cloned. These will introduce additional unmeasured fluctuations, converting a pure input state into a mixed output state [27], consequently leading to a loss of coherence between previously entangled states. We consider eavesdropping on only one of the two channels because, given our emphasis on eavesdropper detection, this is the most advantageous situation for Eve: placing cloners in both channels can only make her situation worse by affecting Alice's state as well.

A generic schematic of a Gaussian cloner is shown in Fig. 2(a). In addition to the input beam to be cloned (represented by annihilation operator $\hat{a}_{\rm in} = \hat{a}_2$), there is an input $\hat{c}_{\rm in}$, assumed to be in a vacuum state, onto which the clone is to be imprinted at output. One further input port $\hat{b}_{\rm in}$ leads to an internal amplifier. We assume the specific model of Ref. [28], realized in terms of two beam splitters and a nondegenerate optical parametric amplifier (NOPA), as in Fig. 2(b). There are three output beams: an ancilla ($\hat{b}_{\rm out}$) and two clones of the input state. One clone ($\hat{a}_{\rm out}$) is sent on to Bob and one ($\hat{c}_{\rm out}$) is kept by Eve. The input-output relations for the operators in the Heisenberg picture are [28]

$$\hat{a}_{\rm out} = \hat{a}_{\rm in} - \frac{e^{-\gamma}}{\sqrt{2}}(\hat{c}_{\rm in} + \hat{b}_{\rm in}^\dagger), \tag{5}$$

$$\hat{b}_{\rm out} = -\sqrt{2}\sinh\gamma\,\hat{c}_{\rm in}^\dagger + \sqrt{2}\gamma\hat{b}_{\rm in} - \hat{a}_{\rm in}^\dagger, \tag{6}$$

$$\hat{c}_{\rm out} = \hat{a}_{\rm in} + \frac{e^{+\gamma}}{\sqrt{2}}(\hat{c}_{\rm in} - \hat{b}_{\rm in}^\dagger). \tag{7}$$

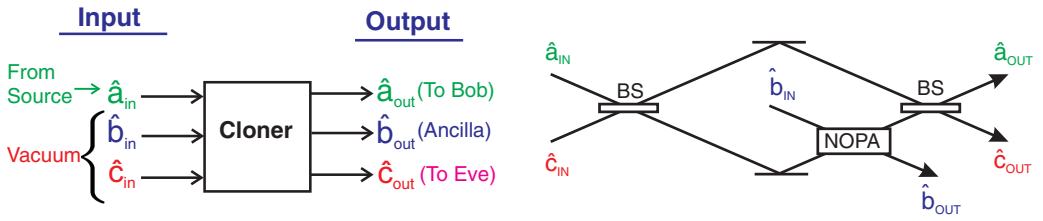


FIG. 2. (Color online) A model of a Gaussian cloner [28] applied by Eve to Bob's beam. The cloner can be realized by combining an amplifier with a beam splitter. Besides the input from the source ($a_{\rm in}$), there are two additional inputs: one to the amplifier ($b_{\rm in}$) and the other to the first beam splitter ($c_{\rm in}$). The result is two outputs with quadratures that have means equal to that of the input. One copy ($a_{\rm out}$) is sent on to Bob. Eve keeps the other ($c_{\rm out}$) to make measurements on.

Here, the asymmetry between the two clones is measured by a parameter ξ which has value $\xi = \frac{\ln 2}{2}$ for the symmetric case. Then, $\gamma = \xi - \frac{\ln 2}{2}$ measures the deviation from symmetry. The optimal case of $\gamma = 0$ produces fidelity $F_a = F_c = \frac{2}{3}$ for both clones. It is readily verified that the mean values at both outputs are unchanged from the input, $\langle \hat{q}_E \rangle = \langle \hat{q}_2' \rangle = \langle \hat{q}_2 \rangle$ and $\langle \hat{p}_E \rangle = \langle \hat{p}_2' \rangle = \langle \hat{p}_2 \rangle$. It is also straightforward to show that the variances satisfy

$$\Delta q^2_{a,\rm out} = \Delta q^2_{a,\rm in} + \tfrac{1}{4} e^{-2\gamma}, \tag{8}$$

$$\Delta p^2_{a,\rm out} = \Delta p^2_{a,\rm in} + \tfrac{1}{4} e^{-2\gamma}, \tag{9}$$

for the clone sent to Bob, and

$$\Delta q^2_{c,\rm out} = \Delta q^2_{c,\rm in} + \tfrac{1}{4} e^{+2\gamma}, \tag{10}$$

$$\Delta p^2_{c,\rm out} = \Delta p^2_{c,\rm in} + \tfrac{1}{4} e^{+2\gamma}, \tag{11}$$

for the clone kept by Eve. Due to the cloning procedure, Bob and Eve each therefore gain added variances (beyond the original variance of the beam in transit to Bob) of $\sigma_B^2 = \frac{1}{4} e^{-2\gamma}$ and $\sigma_E^2 = \frac{1}{4} e^{2\gamma}$, respectively.

In the Schrödinger picture, the cloner has the effect of altering the state: a pure input state will be converted to a mixed output with a probability distribution of width σ_B^2 [27], which will inevitably damage or destroy the entanglement of the cloned state with Alice's state.

Note that in Eqs. (8)–(11), the eavesdropper adds a fixed amount to the variance (regardless of her position), while the incoming variance itself increases with distance, due to mixing with vacuum contributions as loss occurs. As a result, the fractional effect she has is smaller and harder to detect at large distances; but, at the same time, she gains less information, since at larger distances she is measuring something that is already more uncertain. The net result is that it is slightly more favorable from Eve's point of view for her to act closer to the source than to act at larger distances. Therefore, in the following sections, we will always assume that Eve is operating very near the source.

IV. ENTANGLEMENT-WITNESS APPROACH

Recall that by using the Bell–Clauser-Horne-Shimony-Holt (CHSH) inequality, the absolute value of the expectation value of the Bell-CHSH operator $\mathcal{B}$, when properly applied, provides a necessary and sufficient indication of the presence or absence of entanglement for pure states. In that sense, the absolute value $|\mathcal{B}|$ is the longest-used strong entanglement witness. Here, in place of $|\mathcal{B}|$ falling below the critical Bell inequality value 2 as the indicator of loss of entanglement, we use the loss of the negative-valuedness of an entanglement witness $\mathcal{S}$ that is observable with a much simpler apparatus.

An entanglement witness is a quantity which is negative whenever a system is entangled; in general, when it is non-negative this is no longer the case and nothing can be said about the entanglement or separability of the system. Entanglement witnesses can often be based on the positive partial trace (PPT) criterion of [7,29]. For continuous variables, the most common such witnesses are formed from the second-order correlation functions (i.e., on covariance matrices). These are extremely useful because Gaussian states are completely determined by their means and covariance matrices; as a result, such witnesses often completely characterize the entanglement properties of Gaussian states. In particular, some entanglement witnesses, such as the function $\mathcal{W}_s$ mentioned in Sec. V, are both *necessary* and *sufficient* conditions for entanglement when applied to Gaussian states, being positive if *and only if* the state is separable. Such witnesses are referred to as strong witnesses.

However, covariance-based entanglement measures, which do not take into account correlations among higher moments, may not be fine enough a measure to detect entanglement in non-Gaussian systems, so a number of higher-order entanglement measures have been discussed in the literature [9,30–33]. These involve expectation values of operators formed from products of more than two creation or annihilation operators (or, equivalently, products of more than two quadrature operators). Here we will consider one such measure, denoted $\mathcal{S}$, and show that it can detect the presence of eavesdropping: when an eavesdropper acts, it will switch sign from negative to positive values. Because $\mathcal{S} < 0$ is only a sufficient and not a necessary measure for entanglement—in other words, $\mathcal{S}$ is not a strong witness—it cannot be said with certainty that entanglement is lost when the sign changes. Whether or not entanglement persists after the sign change is ultimately beside the point for our current purpose: the sign change in any case indicates the presence of an eavesdropper, which is our goal. In addition, so long as the sign does remain negative, we *can* say with certainty that the system remains entangled, and that under an appropriate protocol it therefore remains secure. If $\mathcal{S} < 0$, then entanglement persists and communication can

continue; but if $\mathcal{S} \geqslant 0$, communication should be shut down in order to assure security, even though there is a chance that entanglement still persists.

The entanglement witness to be used here was introduced in [9] and is defined by the determinant

$$\mathcal{S} = \begin{vmatrix} 1 & \langle \hat{a}_2^\dagger \rangle & \langle \hat{a}_1 \hat{a}_2^\dagger \rangle \\ \langle \hat{a}_2 \rangle & \langle \hat{a}_2^\dagger \hat{a}_2 \rangle & \langle \hat{a}_1 \hat{a}_2^\dagger \hat{a}_2 \rangle \\ \langle \hat{a}_1^\dagger \hat{a}_2 \rangle & \langle \hat{a}_1^\dagger \hat{a}_2^\dagger \hat{a}_2 \rangle & \langle \hat{a}_1^\dagger \hat{a}_1 \hat{a}_2^\dagger \hat{a}_2 \rangle \end{vmatrix}. \tag{12}$$

Here, $\hat{a}_1$ is the annihilation operator at Alice's location and $\hat{a}_2$ is the corresponding operator for Bob's location. This witness is valid for any state, Gaussian or otherwise, and when it is negative, the state is guaranteed to be entangled. Because $\mathcal{S}$ involves third-order correlations in addition to second and fourth order, it is more difficult to measure experimentally, although such measurements have been done [34]. The only change of the setup from Fig. 1(a) is that the homodyne detectors would be replaced by a more complex detection unit.

Given the explicit form of the entangled bipartite coherent state $|\psi\rangle$ given in Eq. (2), $\mathcal{S}$ can be readily calculated. We find the elements of the matrix at zero distance are

$$\langle \hat{a}_2^\dagger \rangle = \langle \hat{a}_2 \rangle = \alpha \cos\phi, \tag{13}$$

$$\langle \hat{a}_1 \hat{a}_2^\dagger \rangle = \langle \hat{a}_1^\dagger \hat{a}_2 \rangle = \alpha^2 |N|^2 (\cos 2\phi + e^{-4\alpha^2 \sin^2\phi}), \tag{14}$$

$$\langle \hat{a}_2^\dagger \hat{a}_2 \rangle = \alpha^2 |N|^2 (1 + \cos 2\phi e^{-4\alpha^2 \sin^2\phi}), \tag{15}$$

$$\langle \hat{a}_1 \hat{a}_2^\dagger \hat{a}_2 \rangle = \alpha^3 \cos\phi, \tag{16}$$

$$\langle \hat{a}_1^\dagger \hat{a}_1 \hat{a}_2^\dagger \hat{a}_2 \rangle = \alpha^4. \tag{17}$$

It is straightforward to verify that $\mathcal{S} \to 0$ as $\alpha \to 0$ or $\alpha \to \infty$, while $\mathcal{S} < 0$ at all finite values of α. All terms in the determinant are proportional to α^6, with additional amplitude dependence coming from the exponential terms in Eqs. (14) and (16); the latter terms are negligible except when $\alpha \ll 1$. For small ϕ, the terms in $\mathcal{S}$ nearly cancel, leaving $\mathcal{S}$ with a small (negative) value. $\mathcal{S} \to 0$ continuously as $\phi \to 0$, i.e., as the state becomes separable.

Distance dependence can be taken into account by replacing the amplitude in each arm by $\alpha \to \alpha_j(d_j) = \alpha t_j(d_k)$, where t_j is a transmission function in the jth branch, for $j = 1,2$. We assume that $\phi \ll 1$ and $\alpha\phi \gg 1$ initially, but due to losses, α will eventually decay to small values, at which point the phase-space regions centered at $\alpha e^{\pm i\phi}$ may begin to overlap, resulting in entanglement loss. For propagation losses alone, the transmission functions are of the form $t_j(d_j) = e^{-\frac{1}{2}K_j d_j}$, with propagation distance d_j in each arm. When these losses are included, expressions of the form $\langle \hat{a}_1^l \hat{a}_1^{\dagger m} \hat{a}_2^n \hat{a}_2^{\dagger p} \rangle$ are multiplied by factors of $e^{-\frac{K}{2}[(l+m)d_1 - (n+p)d_2]}$, while the exponential terms in Eqs. (13)–(17) and in the normalization constant given by Eq. (3) become $\exp(-4\alpha^2 e^{-\frac{K}{2}(d_1+d_2)} \sin^2\phi)$. Given this, the entanglement witness can be calculated as a function of distance for various parameter values.

Plots of $\mathcal{S}$ versus distance are shown in Fig. 3 for several parameter values. Two cases are shown: the case of equal decay in both arms (Alice and Bob equal distances from the source) and for decay in one arm only (Alice acting as the source). Note that for the asymmetric case, $\mathcal{S}$ has been multiplied by 100 in Fig. 3(a) in order to display it on the same scale as the symmetric case. As expected, $\mathcal{S}$ is initially small and negative. As the amplitudes decay, the exponential terms in Eqs. (14) and (15) start to become significant when $\exp(-4\alpha^2 e^{-\frac{K}{2}(d_1+d_2)} \sin^2\phi)$ becomes comparable in size to $\cos 2\phi$. This signals the beginning of significant overlap between the two phase-space regions in Fig. 4. At this point, there is a negative dip in $\mathcal{S}$, followed by an asymptotic decay back toward zero, due to the decay of the overall $\alpha^6(d)$ dependence. The latter decay results from the regions of Fig. 4 approaching the vacuum state at the origin. Thus, the dips occur at the point where the entanglement starts to become unusable due to photon loss, and therefore signals the outer limits of the distance at which the method is useful for the given input parameters.

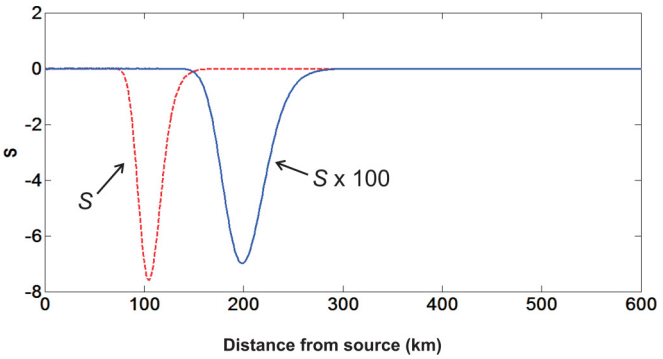


FIG. 3. (Color online) (a) Behavior of entanglement witness $\mathcal{S}$ as a function of distance, assuming that the amplitudes have decay constants $K = 0.046$ km^{-1}. Here, $\alpha = 100$ and $\phi = 0.1$. The red dashed line assumes symmetric decay. The solid blue line assumes that the source is in Alice's laboratory, so that decay occurs only on one side; the values in this latter case were magnified by a factor of 100 before plotting.

Note from the figure that although the large negative dip is orders-of-magnitudes smaller when the decay is occurring in only one arm, it occurs at roughly twice the distance. The zero crossing of $\mathcal{W}$ will similarly be seen in the next section to occur at twice the distance in the asymmetric case. This is significant because it means that the mechanism

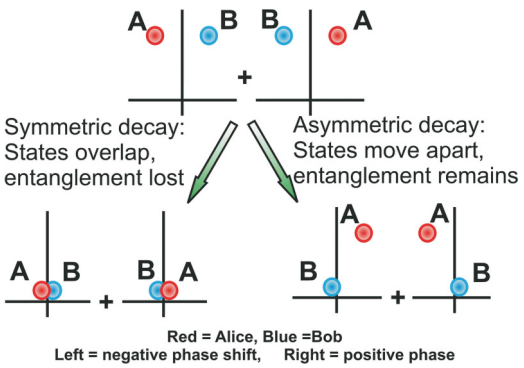


FIG. 4. (Color online) The larger distance of disentanglement for the asymmetric case in Fig. 3 is due to the fact that the two coherent states move apart in phase space, whereas in the symmetric case, both decay toward the same vacuum state.

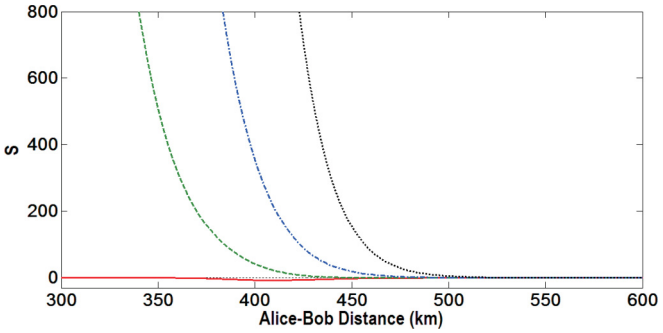


FIG. 5. (Color online) Behavior of entanglement witness $\mathcal{S}$ as a function of distance, with and without eavesdropping, for $\alpha = 1000$ and $\phi = 0.1$, assuming symmetric decay. The curves correspond to no eavesdropping (solid red), $\gamma = 0$ (dashed green), $\gamma = -1$ (dash-dotted blue), and $\gamma = -2$ (dotted black).

for eavesdropper detection will work over roughly twice the distance in the asymmetric case. As shown in Fig. 4, the entanglement loss is slower in the asymmetric case because the two states may initially move apart as one of them approaches the origin more rapidly than the other. In any event, as will be seen in the next section, the dips in $\mathcal{S}$ occur at roughly the location where the photon number has decayed to the point where homodyne measurements become imprecise. Thus, predictions beyond the beginning of these dips should be considered meaningless. Henceforth, except when stated otherwise, the figures in the remainder of this paper will be plotted for the symmetric case versus total Alice-Bob distance, $d = d_1 + d_2$; plotted this way, the asymmetric case shows only minor differences, aside from a change of scale.

Replacing $\hat{a}_2$ in Eq. (12) by the output $\hat{a}_{\text{out}}$ of a cloner, the effect of eavesdropping on $\mathcal{S}$ can be evaluated. Examples of the results are shown in Fig. 5. It is clear from the plots that $\mathcal{S} < 0$ in the absence of eavesdropping, but switches to $\mathcal{S} > 0$ when Eve is present.

Since $\mathcal{S}$ is only slightly negative at most distances, it only requires a small disturbance to tip it to the positive side of the axis. The initially large size of the positive $\mathcal{S}$ values in the presence of eavesdropping may seem surprising, but it can be traced to its source: the large value of $\langle \hat{a}_1^\dagger \hat{a}_1 \rangle$ acts as a multiplier, magnifying changes in $\mathcal{S}$. To see this, note first that if $\mathcal{S}$ is expanded out explicitly in terms of expectation values, the only terms that change when the eavesdropper acts can be written in the form

$$(\langle \hat{a}_1^\dagger \hat{a}_1 \rangle - \langle \hat{a}_1^\dagger \rangle^2) \langle \hat{a}_1^\dagger \hat{a}_1 \hat{a}_2^\dagger \hat{a}_2 \rangle. \tag{18}$$

The terms in the parentheses can be written as $\langle \Delta q_1^2 + \Delta p_1^2 + i[\hat{p}_1, \hat{q}_1] \rangle$, which is non-negative on general quantum mechanical principles; for the specific states considered in this paper, it can be written more concretely as $\alpha^2 \sin^2 \phi$, which is also clearly non-negative. Since this term is positive, $\mathcal{S}$ will increase if the fourth-order term multiplying it increases. With eavesdropping, the fourth-order term *does* increase by an amount proportional to $\langle \hat{a}_1^\dagger \hat{a}_1 \rangle e^{-2\gamma}$, which, in turn, is proportional to Alice's squared amplitude, α^2. At small distances, $\mathcal{S}$ is initially small and negative, but the amplitude α is large, so that this term adds a large positive value to the entanglement witness. In more physical terms, the cloner transforms the initial pure state en route to Bob into a mixed state, leading to a decrease in entanglement; the effect of this loss on the witness is large because it is multiplied by the coherent-state amplitude, which we explicitly assume to be large. The loss of decoherence results from the fact that not only are the phase-space regions in Fig. 4 larger, their locations fluctuate relative to each other about fixed average positions as a result of the uncontrolled relative phase fluctuations introduced by the cloner.

V. AN EAVESDROPPING WITNESS

In analogy to an entanglement witness, we wish now to introduce the concept of an *eavesdropping* witness. We will define this to be an experimentally measurable function of the system's state which changes value in a predictable manner whenever an eavesdropper acts on the system. Here we will introduce such a measure that will give results closely related to those of the entanglement witness $\mathcal{S}$ introduced in Sec. IV. So this function will also witness eavesdropping, but is much easier to measure. This eavesdropping witness $\mathcal{W}$ is constructed from the covariance matrix of the system and will change signs from negative to positive at a distance that can be easily calculated. This distance changes in a predictable manner when the system is interfered with, thus signaling the presence of an eavesdropper.

Let $\hat{q}_1, \hat{p}_1$ be orthogonal quadratures for beam A and $\hat{q}_2, \hat{p}_2$ be corresponding quadratures for B. Form the vector: $\hat{\eta}(\hat{q}_1, \hat{p}_1, \hat{q}_2, \hat{p}_2)$. The *covariance matrix* V is defined as the 4×4 matrix with elements $V_{ij} = \frac{1}{2}\langle \{\hat{\eta}_i - \langle \eta_i \rangle, \hat{\eta}_j - \langle \eta_j \rangle\} \rangle$, where $\{\ldots,\ldots\}$ denotes the anticommutator and angular brackets denote the expectation value. V can be expressed in terms of three 2×2 matrices as $V = \left(\begin{smallmatrix} A_1 & C \\ C^T & A_2 \end{smallmatrix}\right)$. A_1 and A_2 are the self-covariance matrices of each beam separately; C describes correlations between the A_i. An eavesdropping witness derived from the covariance matrix is then defined as

$$\mathcal{W} = 1 + \det V + 2 \det C - \det A_1 - \det A_2. \tag{19}$$

This function $\mathcal{W}$ is similar in form to an entanglement witness $\mathcal{W}_s$ introduced in [17] and studied in detail in [18], but due to the normalization differences mentioned in the introduction, it is not the same function and so here is not a true entanglement witness. $\mathcal{W}$ and $\mathcal{W}_s$ are, in fact, related by a rescaling of the quadratures, but for the states considered in this paper, $\mathcal{W}_s$ vanishes identically. It can be shown that for Gaussian states, a system is entangled if and only if $\mathcal{W}_s < 0$. $\mathcal{W}_s$, like $\mathcal{S}$, is based on the positive partial trace criterion [7,29]; however, because $\mathcal{W}_s$ is quadratic in the quadrature operators, it is unable to detect some forms of entanglement that can be detected by the quartic operator $\mathcal{S}$. The vanishing of $\mathcal{W}_s$ on the states used here is due to the fact that they are not strictly Gaussian; however, we will make use in Sec. VII of the fact that the non-Gaussian terms are small for large α.

Using an eavesdropping witness derived from the covariance matrix, as $\mathcal{W}$ is, has distinct advantages, since V is experimentally measurable via heterodyne detection and its expected behavior with distance is straightforward to calculate. So deviations from its expected distance dependence are easily detected. The eavesdropper's actions affect the various

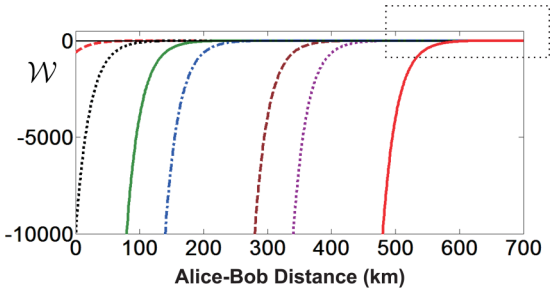


FIG. 6. (Color online) Eavesdropping witness $\mathcal{W}$ value vs Alice-Bob distance $d = d_1 + d_2$. From left to right, the curves have parameter values $|\alpha\phi| = 10$, $|\alpha\phi| = 20$, $|\alpha\phi| = 50$, $|\alpha\phi| = 100$, $|\alpha\phi| = 500$, $|\alpha\phi| = 1000$, and $|\alpha\phi| = 5000$. $K = 0.046$ km^{-1} is used for the 1550 nm telecom window. An expanded view of the region enclosed in the dashed box is shown in Fig. 7.

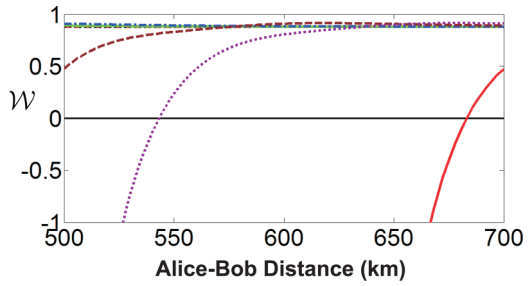


FIG. 7. (Color online) Expanded view of the region enclosed in the dashed box in Fig. 6. The curves have parameter values $|\alpha\phi| = 500$ (dashed brown), $|\alpha\phi| = 1000$ (dotted violet), and $|\alpha\phi| = 5000$ (solid red). $K = 0.046\,\mathrm{km}^{-1}$ is used for the 1550 nm telecom window.

covariances and moments of the states; the idea is to find a function which distills these effects into a single number in a useful way. Clearly, many such functions are possible, but we examine here just one example.

Assuming loss rates K_1 and K_2 in each arm, the covariance matrix is

$$V = \begin{pmatrix} A_1' & C' \\ C'^{\,T} & A_2' \end{pmatrix} = \begin{pmatrix} a_1' & 0 & b' & 0 \\ 0 & a_1' & 0 & c' \\ b' & 0 & a_2' & 0 \\ 0 & c' & 0 & a_2' \end{pmatrix}, \tag{20}$$

where

$$a_j'(d_j) = \frac{|\alpha|^2}{2}[|N|^2 f(\theta,\phi,d_j) - 1]e^{-K_j d_j} + \frac{1}{4}, \tag{21}$$

$$b'(d_1,d_2) = \frac{|\alpha|^2}{2}[|N|^2 g(\theta,\phi,d_1,d_2) - \cos 2\phi] \times e^{-\frac{1}{2}(K_1 d_1 + K_2 d_2)}, \tag{22}$$

$$c'(d_1,d_2) = \frac{|\alpha|^2}{2}[|N|^2 g(\theta,\phi,d_1,d_2) - 1]e^{-\frac{1}{2}(K_1 d_1 + K_2 d_2)}, \tag{23}$$

with $j = 1,2$. Here we have also defined

$$f(\theta,\phi,d_j) = [1 + \cos 2\phi \cos\theta e^{-4|\alpha|^2 \sin^2\phi e^{-Kd_j}}],$$
$$g(\theta,\phi,d_1,d_2) = [\cos 2\phi + \cos\theta e^{-4|\alpha|^2 \sin^2\phi e^{-(K_1 d_1 + K_2 d_2)/2}}]. \tag{24}$$

The values of a', b', c' at zero distance will be denoted by a, b, c. Distance dependence also arises through $N(d_1,d_2)$. The entanglement witness is then

$$\mathcal{W} = 1 + (a_1' a_2')^2 + (b'c')^2 - (b'^2 + c'^2)a_1' a_2' + 2b'c' - a_1'^2 - a_2'^2. \tag{25}$$

Henceforth we assume that in both channels, the rate for fiber loss is that of the 1550 nm telecom window, $K_1 = K_2 \equiv K = 0.046$ km^{-1}, corresponding to 3 dB loss per 15 km. Now we also, for the most part, express results in terms of the total Alice-to-Bob distance, $d = d_1 + d_2$. In this manner, the symmetric case (equal travel distances in both channels, $d_1 = d_2$) and the case where Alice generates the state in her laboratory ($d_1 = 0$, with no losses on her side) can both be expressed in a unified manner. Plots of $\mathcal{W}$ vs distance are given in Fig. 6. $\mathcal{W}$ starts with large negative values at $d = 0$ and its magnitude decays rapidly with distance due to propagation losses. Close inspection shows that $\mathcal{W}$ crosses from negative to positive values at finite distances (see the expanded version in Fig. 7).

The exponential terms in f and g are negligible except at large distances, by which point the $\alpha^2(d)$ terms that multiply them in Eqs. (21)–(23) have decayed away. As a result, these terms can be neglected for most purposes. Dropping them, it is then seen that all of the curves in Fig. 7 converge to a common asymptote as $|\alpha| \to \infty$, located at $\mathcal{W} = (1 - a^2)^2 = (\frac{15}{16})^2 \approx 0.8789$.

VI. CROSSING THRESHOLDS

Entanglement sudden death (ESD) is the sudden loss of entanglement in finite time—corresponding here to finite distance—in contrast to the more common asymptotic loss of entanglement due to decoherence [19,35,36]. Although, as mentioned, the eavesdropping witness $\mathcal{W}$ is not an entanglement witness, behavior analogous to ESD occurs here. The point at which the axis is crossed moves in the presence of eavesdropping and closely tracks features of the true entanglement $\mathcal{S}$ witness discussed in Sec. IV; as a result, the location of this crossing point can be used as a means of eavesdropper detection.

For $\phi = 0$, the matrix elements reduce to $a = \frac{1}{4}$ and $b = c = 0$, so we find that $\mathcal{W} = 1 - a^4 - 2a^2 = (1 - a^2)^2 = (\frac{15}{16})^2 > 0$, at all distances. But for nonzero ϕ, $\mathcal{W}$ changes sign when $|\alpha(d)| = \sqrt{\frac{15}{4}}\,\csc\phi$. Solving for distance, we find that the sign change occurs when the distance between Alice and Bob is

$$d_0 = \frac{2}{K}\ln\left(\sqrt{\frac{8}{15}}\alpha\sin\phi\right). \tag{26}$$

These results are plotted in Fig. 8. Although here we restrict ourselves to small ϕ, it may be noted in passing that, for fixed α, the crossing distance is largest at $\phi = \frac{\pi}{2}$, i.e., when the entangled states are $|\alpha\rangle$ and $|-\alpha\rangle$. As the distance formula makes clear, crossing can always be made to occur at any distance desired by choosing appropriate values of ϕ and α.

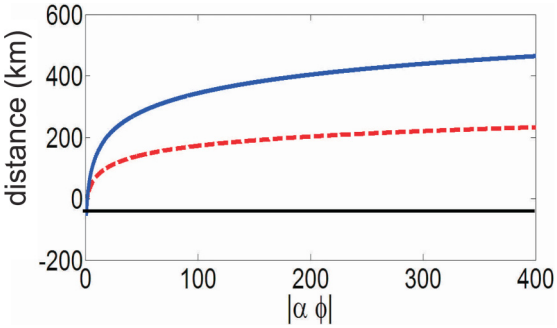


FIG. 8. (Color online) The distance d_0 at which axis crossing occurs, as a function of the parameter $|\alpha\phi| \approx |\alpha \sin\phi|$ for $K = 0.046\,\mathrm{km}^{-1}$. The solid blue curve is the Alice-to-Bob distance. This is the same as the source-to-Bob distance for the case of loss in only one arm (source in Alice's laboratory), and is double the source-to-Bob distance for case of equal distances in both branches (dashed red curve).

Let us now consider the effect of eavesdropping on $\mathcal{W}$. The variances on the diagonal of A_2 are increased by $\frac{1}{4}e^{-2\gamma}$, so the crossing distance is now altered in the presence of eavesdropping to the value

$$d(\gamma) = \frac{2}{K}\ln\left[\sqrt{\frac{8}{15}}\left(1-\frac{1}{15}e^{-2\gamma}\right)^{-1}\alpha^2\sin^2\phi\right]. \quad (27)$$

Here, $d(\gamma)$ becomes complex for $\gamma < \gamma_0$, where $\gamma_0 \equiv -\frac{1}{2}\ln 15 \approx -1.3540$. So for eavesdropping parameters below γ_0, there is no crossing and $\mathcal{W}$ is always negative. This lack of axis crossing provides a clear and unambiguous signal of eavesdropping. For $\gamma > \gamma_0$, the crossing distance becomes finite, starting at large values and decaying rapidly to d_0 as γ increases (Fig. 9). Since the ratio of Eve's added variance (beyond the vacuum value) to Bob's added variance, $r = \frac{\sigma_E^2}{\sigma_B^2} = e^{4\gamma}$, increases exponentially with γ, the shift in crossing point is large (or infinite) for parameter values where Eve can measure the quadratures with precision (large negative γ). The shift only becomes too small to detect exactly in the region where Eve's variance is too large for her to extract an accurate measurement (positive γ). This is illustrated in

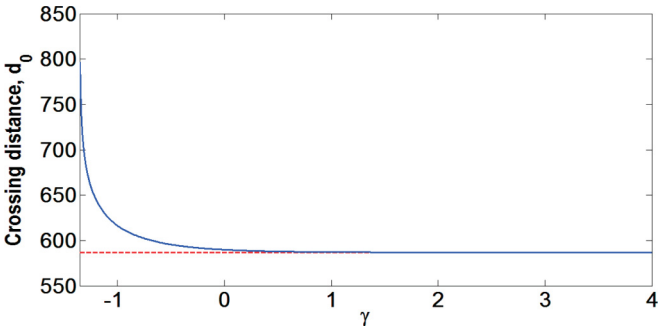


FIG. 9. (Color online) The solid blue line is the distance $d(\gamma)$ (in kilometers) between Alice and Bob at which $\mathcal{W}$ crosses the axis, as a function of eavesdropping parameter γ. The amplitude and phase values assumed are $\alpha = 10^5$ and $\phi = 0.1$. The dashed red line shows the distance d_0 in the absence of eavesdropping.

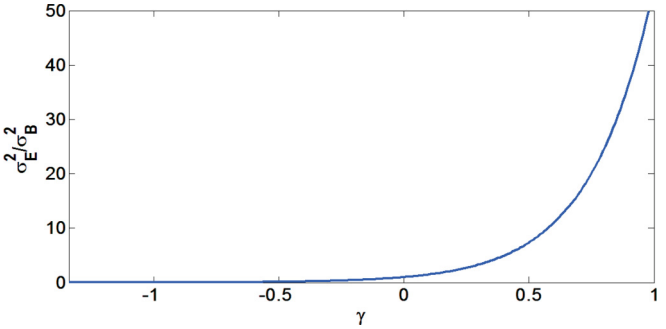


FIG. 10. (Color online) The ratio of added variances for Bob and Eve, $r = \frac{\sigma_E^2}{\sigma_B^2}$, is plotted vs γ, for $\phi = 0.1$. The curve is independent of α.

Fig. 10, where r is plotted versus γ. By the time the shift in crossing point is reduced to 1 meter in size, Eve's variance is 2.2 times that of Bob's variance; by the time Δd drops to 0.5 meters, the added variance ratio grows to $r = 8.6$ (see Fig. 11).

The average number of photons in a coherent state is related to the amplitude by $\langle n\rangle = \alpha^2$, so if the amplitude is decaying as $\alpha(d) = \alpha e^{-Kd/2}$, then the distance D_1 at which the number of photons decays to roughly one is

$$D_1 = \frac{2}{K}\ln\alpha. \quad (28)$$

More generally, the distance at which the number has decayed to $\langle n\rangle = N$ is

$$D_N = \frac{2}{K}\ln\left(\frac{\alpha}{\sqrt{N}}\right). \quad (29)$$

Unless ϕ is relatively large (of the order of 0.1 or more), the points at which the curves cross the axis tend to be in the regions where a small number of photons remain in the beam, making homodyne or heterodyne measurements at those points imprecise. As a result, it is advantageous instead to look at the distances at which the $\mathcal{W}$ curve crosses some negative value Λ, instead of the distance where it crosses zero. Let the distance at which $\mathcal{W} = \Lambda$ be $d(\gamma,\Lambda)$. In the

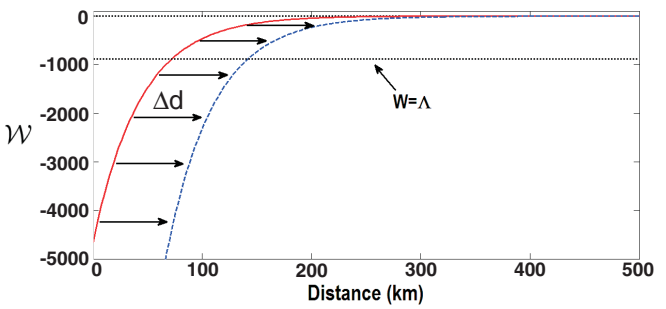


FIG. 11. (Color online) The curves shift horizontally by approximately a constant amount $\Delta d(\gamma,\Lambda)$ in the presence of eavesdropping. Here the solid red line is in the absence of eavesdropping for $\alpha = 1000$ and $\phi = 0.1$. The dashed blue line is in the presence of eavesdropping with $\gamma = -1$. The crossing of the $\mathcal{W} = \Lambda$ line can be used instead of the $\mathcal{W} = 0$ crossing; this allows more photons to still be present for measurement, increasing measurement accuracy.

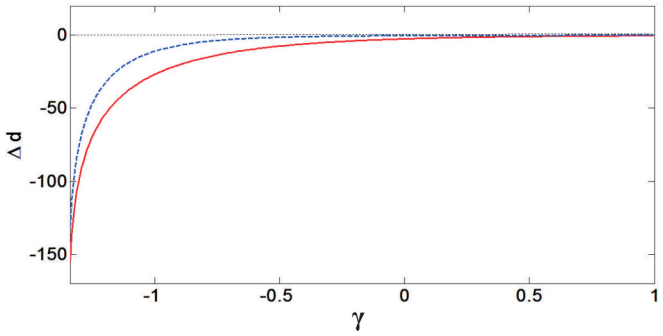


FIG. 12. (Color online) The change Δd in the distance at which the curve of $\mathcal{W}$ crosses the value $\mathcal{W}$ is plotted vs the eavesdropping parameter γ, for the values $\Lambda = -1$ (dashed blue) and $\Lambda = -10$ (solid red). The curves are independent of α and change very little for $\Lambda < -10$. The value $\phi = 0.1$ was used for the plots.

absence of an eavesdropper, the distance would be $d(\infty,\Lambda)$, so that the distance that this crossing moves in the presence of eavesdropping is $\Delta d(\gamma,\Lambda) = d(\gamma,\Lambda) - d(\infty,\Lambda)$. It is straightforward to show that

$$d(\gamma,\Lambda) = \frac{2}{K}\ln\left[\frac{\alpha^2\sin^2\phi}{F(\gamma)-\frac{\Lambda}{F(\gamma)}}\right], \tag{30}$$

$$\Delta d(\gamma,\Lambda) = \frac{2}{K}\ln\left[\frac{\frac{15}{16}-\frac{16}{15}\Lambda}{F(\gamma)-\frac{\Lambda}{F(\gamma)}}\right], \tag{31}$$

where $F(\gamma) \equiv \frac{15}{16}(1-\frac{1}{15}e^{-2\gamma})$. This shift is independent of the initial value of α and varies only very slowly with Λ. The value of Λ used can be chosen as appropriate for the given experiment to ensure that there are still sufficient numbers of photons remaining in the beam for accurate homodyne measurements. The size of this shift for the particular values $\Lambda = -1$ and $\Lambda = -10$ is shown in Fig. 12. For more negative values of Λ, the curves are nearly indistinguishable from that of $\Lambda = -10$.

Finally, in a fully practical setting, the easiest approach would be to monitor changes of $\mathcal{W}$ at a fixed distance, rather than move the detector around to find a fixed value of $\mathcal{W}$. Since the expected value of $\mathcal{W}$ in the absence of eavesdropping is readily calculable, this is equivalent to the approach described here.

VII. INFORMATION AND SECRET-KEY RATE

Although the primary goal in this paper is to use entanglement in the phase in order to detect eavesdropping on a classically modulated channel, rather than to use the entangled phase for encryption or encoding itself, we briefly consider here other possibilities which are available in case a full quantum key distribution is desired.

In particular, the same setup can be used to generate a key from the homodyne measurements themselves. The possible phase values measured by each participant can be divided up into bins and the bin in which a measurement falls then determines a value for the key. In this situation, the mutual information between the participants and the eavesdropper is relevant to determining if it is possible to distill a secret key. With a sufficient number of bins, the phase variable can still be treated as approximately continuous.

The secret-key rate is given by

$$\kappa = I(A:B) - I(B:E), \tag{32}$$

where $I(A:B)$ and $I(B:E)$ are, respectively, the mutual information between Alice and Bob and between Bob and Eve. The mutual information is simply the difference between the von Neumann entropies of the individual subsystems and the total two-beam system, $S_{vn} = -\mathrm{Tr}\,[\rho\ln\rho]$; for example, $I(A:B) = S_{vn}(\rho_A) + S_{vn}(\rho_B) - S_{vn}(\rho_{AB})$. If $K > 0$, then it is possible to distill a secret key via privacy amplification. If the difference in Eq. (32) is negative, then κ is taken to be zero. The mutual information can be calculated numerically from the density operator of the system. However, an approximate but simpler and more transparent evaluation can be obtained by noting that the system in question can be treated as an approximately Gaussian system for small ϕ. This can be seen, for example, by calculating the characteristic function (the Fourier transform of the Weyl operator) or the Wigner function of the system. The characteristic function, for example, is of the form

$$\begin{aligned}\chi(\lambda,\zeta) = \frac{1}{2}e^{-\frac{1}{4}(|q_1+i\zeta_1|^2+|q_2+i\zeta_2|^2)} &\\ \times\int d^2\lambda d^2\chi\, e^{-(2|\alpha|^2+|\lambda|^2+|\chi|^2)} &\\ \times e^{\frac{i}{2}[(q_1+i\zeta_1)\lambda^*+(q_2+i\zeta_2)\chi^*+(q_1-i\zeta_1)\lambda+(q_2-i\zeta_2)\chi]} &\\ \times(e^{\alpha(\lambda_r+\chi_r)\cos\phi+2\alpha(\lambda_i-\chi_i)\sin\phi} &\\ + e^{\alpha(\lambda_r+\chi_r)\cos\phi+2\alpha(\chi_i-\lambda_i)\sin\phi} &\\ + e^{\alpha(\lambda_r+\chi_r)\cos\phi+2i\alpha(\chi_r-\lambda_r)\sin\phi} &\\ + e^{\alpha(\lambda_r+\chi_r)\cos\phi+2\alpha(\chi_r-\lambda_r)\sin\phi}).\end{aligned} \tag{33}$$

Here, subscripts 1 and 2 label Alice's and Bob's sides, while subscripts r and i label the real and imaginary parts. Because of the terms in the last large parentheses, χ is a sum of four Gaussians. But when ϕ is small, the sine terms in the exponentials become negligible compared to the cosine terms, leaving all four of these terms equal. The only case when this argument breaks down is when the differences $\chi_i - \lambda_i$ or $\chi_r - \lambda_r$ are large; however, this part of the integration range is strongly suppressed by the term $e^{-(2|\alpha|^2+|\lambda|^2+|\chi|^2)}$ in the second line. Thus, to a high degree of accuracy, we can treat the system as Gaussian. This approximation becomes better as the distance becomes large and the amplitudes decay to small values, which is exactly the region of greatest interest to us. We therefore compute all information-related quantities in the Gaussian approximation.

For a two-mode Gaussian state, the mutual information can be obtained directly from the covariance matrix. Define the binary entropy function $h(x) = (x+\frac{1}{4})\ln(x+\frac{1}{4}) + (x-\frac{1}{4})\ln(x-\frac{1}{4})$ and the discriminant of the covariance matrix $\Delta = \det(A) + \det(B) + 2\det(C)$. Then the quantum mutual information is [37,38]

$$I(A:B) = h(\sqrt{\det(A)}) + h(\sqrt{\det(B)}) - h(d_+) - h(d_-), \tag{34}$$

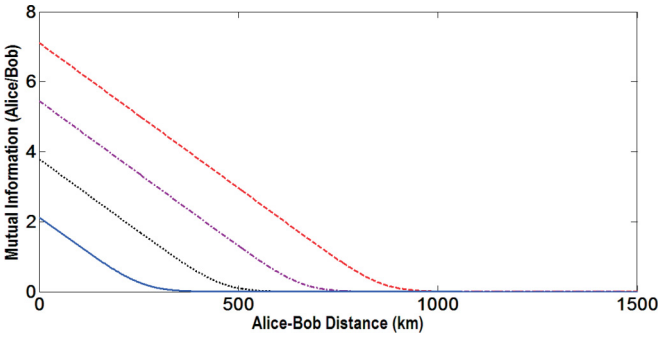


FIG. 13. (Color online) Mutual information between Alice and Bob, assuming both have the same initial amplitude α. From the top line downward, the initial amplitudes are $\alpha = 10^5$ (red), $\alpha = 10^4$ (violet), $\alpha = 10^3$ (black), and $\alpha = 100$ (blue). $\phi = 0.1$ for all curves.

where the symplectic eigenvalues of the covariance matrix are

$$d_{\pm} = \sqrt{\frac{\Delta \pm \sqrt{\Delta^2 - \sqrt{\Delta^2 - 4\det(V)}}}{2}}. \tag{35}$$

Plots of the mutual information between Alice and Bob in the absence of eavesdropping in Fig. 13. In the presence of eavesdropping, examples are shown in Fig. 14. As would be expected, the mutual information they share decreases as γ decreases, i.e., as Bob's variance increases and Eve's drops. Because of the relation between Bob's variance and Eve's variance, it can be noted that the mutual information between Alice and Eve is given by the same formula, but with the sign of γ reversed. This makes calculating the secret-key rate very simple and leads to results such as those shown in Fig. 15. The key rate remains positive as long as $\gamma > 0$, which is equivalent to saying $\sigma_E^2 > \sigma_B^2$. It should be noted that the distances at which the information approaches zero are roughly equal to the distances at which $\mathcal{S}$ became small in Sec. IV. Since $\gamma = 0$ corresponds to $\sigma_E^2 = \frac{1}{4}$, it follows that the maximum allowed noise in the system for arrangement to remain secure is $\sigma^2_{\text{noise}} < \frac{1}{4}$.

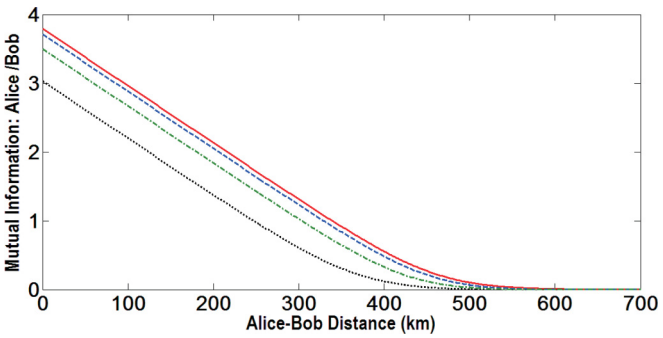


FIG. 14. (Color online) Mutual information between Alice and Bob in the presence of eavesdropping, assuming they have equal initial amplitudes and equal losses. Solid red curve: no eavesdropper. Dotted black curve: $\gamma = -1$. Dash-dotted green curve: $\gamma = 0$. Dashed blue curve: $\gamma = 1$. The values $\phi = 0.1$ and $\alpha = 1000$ were used for all curves. The same curves give the mutual information between Bob and Eve, but with γ and $-\gamma$ interchanged.

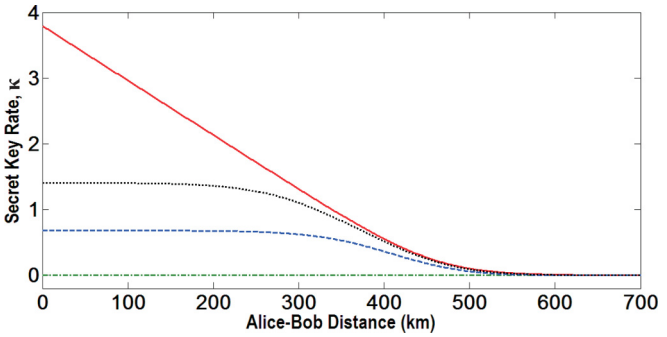


FIG. 15. (Color online) Secret-key rate κ between Alice and Bob in the presence of eavesdropping, assuming they have equal initial amplitudes and equal losses. Solid red curve: no eavesdropper. Dotted black curve: $\gamma = 2$. Dashed blue curve: $\gamma = 1$. Dash-dotted green curve: $\gamma = 0$. κ vanishes identically for all $\gamma \leqslant 0$. The values $\phi = 0.1$ and $\alpha = 1000$ were used for all curves.

As an interesting aside, up to this point, although different amounts of loss were allowed in Alice's and Bob's channels due to different propagation distances, it has always been assumed that the initial amplitudes were equal for both lines. If we allow different initial amplitudes α and β, respectively, for Alice and Bob, then the information decreases more slowly with distance (Fig. 16). The reason for this is similar to the explanation given earlier (see Fig. 4) for the greater distance in the presence of asymmetric decay.

VIII. CONCLUSIONS

We have analyzed the effects of loss and eavesdropping in a system for distributing key bits via entangled coherent states over long distances. We have demonstrated that when combined with the entanglement-witness or eavesdropping-witness approach, the entangled coherent-state scheme described here can, in principle, be used to detect eavesdropping over distances on the order of hundreds of kilometers.

Besides differing conceptually from previous approaches, our results for coherent-state QKD based on the use of an entanglement and eavesdropping witnesses for eavesdropper detection offer distinct advantages over the use of a Bell-type

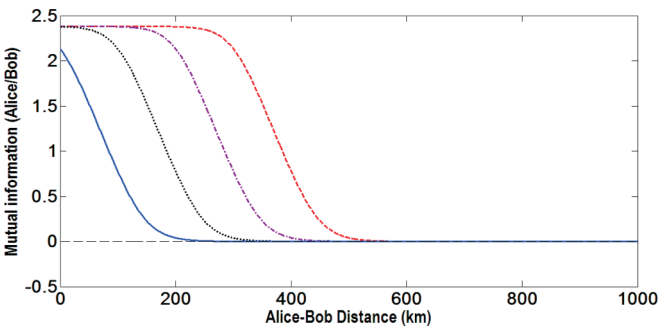


FIG. 16. (Color online) Mutual information between Alice and Bob, assuming they have different initial amplitudes α and β. From the right to left, Bob's initial amplitudes are $\beta = 10^5$ (red), $\beta = 10^4$ (violet), $\beta = 10^3$ (black), and $\beta = 100$ (blue). $\phi = 0.1$ and $\alpha = 100$ for all curves.

inequality for that purpose. In particular, comparing the above results with those in [6], we see that sign changes of $\mathcal{W}$ always occur at larger distances than the loss of Bell nonlocality resulting from the same external interventions on the induced coherent states. Hence, $\mathcal{W}$, as well as $\mathcal{S}$, is available for eavesdropping detection over larger distances than the Bell-type inequality of the proposal in [6], extending the range of distances in which the phase-entangled coherent states are known to be useful for QKD: simulations in [6] showed the Bell inequality method to be useful up to distances on the order of tens of kilometers, while the method discussed below has promise to extend the range to the order of several hundred kilometers. Moreover, the entanglement-witness method requires only a single trigger photon, rather than the triple-coincidence trigger required for testing the Bell-type inequality, a substantial practical improvement.

Of the two eavesdropping witnesses, one ($\mathcal{W}$) is straightforward to implement experimentally, while the other ($\mathcal{S}$) provides a rigorous measure of entanglement loss in the presence of eavesdropping. The question remains as to whether there is some other measure that provides both features for this system: a true entanglement witness that is readily accessible experimentally. It would be of particular interest to find a *strong* entanglement witness that would serve this purpose. In any case, the general idea of using an entanglement witness or some related function as an eavesdropping witness or quantum tripwire for eavesdroppers can certainly be exported to communication systems beyond the specific entangled coherent-state system considered here.

Finally, we have shown that the method is potentially useful up to distances of hundreds of kilometers, in contrast to methods based on single-photon communication which are restricted to distances of tens of kilometers at most. It remains to be seen if the method may be combined with the use of quantum repeaters [39] in order to extend the working distance to even greater lengths.

ACKNOWLEDGMENTS

This research was supported by the DARPA QUINESS program through U.S. Army Research Office Award No. W31P4Q-12-1-0015. We would like to thank Prof. N. Lütkenhaus for a very helpful discussion.

[1] 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), pp. 175–179.
[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[3] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[4] B. C. Sanders, Phys. Rev. A **45**, 6811 (1992).
[5] D. A. Rice, G. Jaeger, and B. C. Sanders, Phys. Rev. A **62**, 012101 (2000).
[6] B. T. Kirby and J. D. Franson, Phys. Rev. A **87**, 053822 (2013).
[7] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 1 (1996).
[8] Lu-Ming Duan, G. Giedke, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **84**, 2722 (2000).
[9] E. Shchukin and W. Vogel, Phys. Rev. Lett. **95**, 230502 (2005).
[10] T. C. Ralph, Phys. Rev. A **61**, 010303(R) (1999).
[11] M. Hillery, Phys. Rev. A **61**, 022309 (2000).
[12] M. D. Reid, Phys. Rev. A **62**, 062308 (2000).
[13] N. J. Cerf, M. Lévy, and G. Van Assche, Phys. Rev. A **63**, 052311 (2001).
[14] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).
[15] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **93**, 170504 (2004).
[16] R. García-Patrón, Ph.D. thesis, Université Libre de Bruxelles, 2007.
[17] R. Simon, Phys. Rev. Lett. **84**, 2726 (2000).
[18] F. A. S. Barbosa, A. J. de Faria, A. S. Coelho, K. N. Cassemiro, A. S. Villar, P. Nussenzveig, and M. Martinelli, Phys. Rev. A **84**, 052330 (2011).
[19] K. Ann and G. Jaeger, Found. Phys. **39**, 790 (2009).
[20] K. Nemoto and W. J. Munro, Phys. Rev. Lett. **93**, 250502 (2004).
[21] W. J. Munro, K. Nemoto, and T. P. Spiller, New J. Phys. **7**, 137 (2005).
[22] M. D. Lukin and A. Imamoglu, Phys. Rev. Lett. **84**, 1419 (2000).
[23] S. E. Harris, J. E. Field, and A. Imamoglu, Phys. Rev. Lett. **64**, 1107 (1990).
[24] H. Schmidt and A. Imamoglu, Opt. Lett. **21**, 1936 (1996).
[25] Q. A. Turchette, C. J. Hood, W. Lange, H. Mabuchi, and H. J. Kimble, Phys. Rev. Lett. **75**, 4710 (1995).
[26] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).
[27] N. J. Cerf, A. Ipe, and X. Rottenberg, Phys. Rev. Lett. **85**, 1754 (2000).
[28] J. Fiurášek, Phys. Rev. Lett. **86**, 4942 (2001).
[29] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).
[30] S. Mancini, V. Giovannetti, D. Vitali, and P. Tombesi, Phys. Rev. Lett. **88**, 120401 (2002).
[31] G. S. Agarwal and A. Biswas, J. Opt. B **7**, 350 (2005).
[32] M. G. Raymer, A. C. Funk, B. C. Sanders, and H. de Guise, Phys. Rev. A **67**, 052104 (2003).
[33] R. M. Gomes, A. Salles, F. Toscano, P. H. Souto Ribeiro, and S. P. Walborn, Proc. Nat. Acad. Sci. USA **106**, 21517 (2009).
[34] L. Dahlström and B. Källsberg, Opt. Commun. **4**, 285 (1971).
[35] T. Yu and J. H. Eberly, Science **323**, 598 (2009).
[36] M. P. Almeida, F. de Melo, M. Hor-Meyll, A. Salles, S. P. Walborn, P. H. Souto Ribeiro, and L. Davidovich, Science **316**, 579 (2007).
[37] S. Olivares, Eur. Phys. J. Spec. Top. **203**, 3 (2012).
[38] A. Serafini, F. Illuminati, and S. De Siena, J. Phys. B: At. Mol. Opt. Phys. **37**, L21 (2004).
[39] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998).