Distinguishability of Gaussian states in quantum cryptography using postselection

Christian Weedbrook,[1],[*] Daniel J. Alton,[2],[†] Thomas Symul,[2] Ping Koy Lam,[2] and Timothy C. Ralph[1]

[1]*Department of Physics, University of Queensland, St. Lucia, Queensland 4072, Australia*

[2]*Department of Physics, Quantum Optics Group, Faculty of Science, Australian National University,*

Australian Capital Territory 0200, Australia

(Received 4 March 2009; published 15 June 2009)

We consider the distinguishability of Gaussian states from the viewpoint of continuous-variable quantum cryptography using postselection. Specifically, we use the probability of error to distinguish between two pure coherent (squeezed) and two particular mixed symmetric coherent (squeezed) states where each mixed state is an incoherent mixture of two pure coherent (squeezed) states with equal and opposite displacements in the conjugate quadrature. We show that the two mixed symmetric Gaussian states (where the various components have the same real part) never give an eavesdropper more information than the two pure Gaussian states. Furthermore, when considering the distinguishability of squeezed states, we show that varying the amount of squeezing leads to a "squeezing" and "antisqueezing" of the net information rates.

I. INTRODUCTION

The laws of quantum mechanics tell us that in general it is impossible to perfectly distinguish between two nonorthogonal quantum states [1]. This limitation imposed by quantum measurement theory [2] is inherent in a number of continuous-variable (CV) quantum information [3] applications, including quantum cloning and the security of quantum cryptography protocols (e.g., see [4]). Closely related to this is quantum state discrimination [5,6], which is concerned with the distinguishability of quantum states. There are two commonly used distinguishability techniques [5,6]: (1) minimum error discrimination and (2) unambiguous state discrimination. In minimum error discrimination, a number of approaches have been developed where quantum states can be distinguished provided we allow a certain amount of uncertainty or error in the measurement results. On the other hand, unambiguous state discrimination is an error-free discrimination process but relies on the fact that sometimes the observer gets an inconclusive result.

Previous work on the distinguishability of CV quantum states includes calculating the Bures distance between two (displaced) squeezed thermal states [7,8], unambiguous discrimination of symmetric coherent states [9] using linear optics [10], binary optical communication for single and entangled modes in realistic channels [11], distinguishing single-mode Gaussian states using homodyne detection [12], coherent state estimation with minimal disturbance [13], using the quantum Chernoff bound as the distinguishability measure [14], and computable bounds for Gaussian state discrimination [15]. Furthermore, various techniques for optimally distinguishing pure optical coherent states with minimum error have been investigated theoretically [16–21] and also experimentally [22,23].

In this paper, we consider a specific distinguishability situation in terms of the CV distinguishability of Gaussian states (in particular coherent and squeezed states) from the viewpoint of CV quantum key distribution (CV-QKD) [24–28]. The security of CV-QKD is fundamentally based on the inability of an eavesdropper to perfectly distinguish between nonorthogonal quantum states [1]. Here we look at how much information a potential eavesdropper can gain when trying to distinguish between two pure coherent states as opposed to distinguishing between two mixed coherent states where each mixed state is an incoherent mixture of two pure coherent states with equal and opposite displacements in the conjugate quadrature. This is of particular interest in CV-QKD schemes, which use the original postselection protocol [26], where it is often accepted that an eavesdropper's knowledge can be upper bounded by assuming that she obtains more information in the case of distinguishing between two pure coherent states than two mixed coherent states of equal phase-space separation [26,29–31]. It may have been anticipated that, given our particular distinguishability configuration in phase space, two mixed coherent states might be more distinguishable than two pure coherent states. However, this is not the case and, consequently, we show that this assumption in postselection-based CV-QKD is valid. In addition, we extend the coherent state case to include the distinguishability of squeezed states. We show that a squeezing and antisqueezing of the net information rates occurs when varying the amount of squeezing. Furthermore, we see the effect (for both coherent and squeezed states) that after a certain amount of phase-space separation the two mixed Gaussian states start "behaving" like the two pure Gaussian states in that the amount of information in distinguishing them both is equal. We also briefly compare the probability of errors from using an optimal positive operator-valued measure (POVM) (which corresponds to our distinguishability measure) to the more practical, and commonly used, quadrature projective measurement.

This paper is structured as follows. In Sec. II we introduce the probability of error as our measure of distinguishability. Sections III and IV analyze the distinguishability of pure and

---

*christian.weedbrook@gmail.com

†Present address: Norman Bridge Laboratory of Physics 12-33, California Institute of Technology, Pasadena, California 91125, USA.

mixed coherent and squeezed states, respectively. Finally, Sec. V offers a discussion with concluding remarks.

II. DISTINGUISHABILITY MEASURE

In this section we introduce our measure of distinguishability of CV quantum states: the probability of error p_e. We point out that there are other quantum distinguishability measures including the Kolmogorov distance, the Bhattacharyya coefficient, and the Shannon distinguishability (for a review of these measures, see e.g., Fuchs and van de Graaf [32]).

A. Probability of error

A benefit of the probability of error is that it is related to the trace norm distance, or simply the trace distance D, between the two density matrices of the states being distinguished and hence can be readily calculated. Furthermore, the corresponding Shannon information can be determined directly from the probability of error measure as we will soon see. It was originally shown by Helstrom [2] that the probability of error between two density matrices is minimized by performing an optimal positive operator-valued measure (POVM) $\mathcal{E}$ [1]. The probability of error is defined as [32]

$$p_e(\rho_0, \rho_1) \overset{\text{def}}{=} \min_{\mathcal{E} \in \mathcal{M}} p_e(\rho_0(\mathcal{E}), \rho_1(\mathcal{E})), \tag{1}$$

where ρ_0 and ρ_1 are two arbitrary density matrices and the POVM takes into account all measurements $\mathcal{M}$. Helstrom showed [2] that the probability of error can be expressed explicitly as

$$p_e(\rho_0, \rho_1) = \frac{1}{2} + \frac{1}{2} \sum_{\lambda_j \leq 0} \lambda_j, \tag{2}$$

where λ_j are the eigenvalues of the matrix $\rho_0 - \rho_1$. It was shown in [32] that the above could be rewritten as

$$p_e(\rho_0, \rho_1) = \frac{1}{2} - \frac{1}{4} \sum_{j=1}^{N} |\lambda_j|, \tag{3}$$

where the summation is over all eigenvalues. Using this, the probability of error can be alternatively expressed as [2]

$$p_e = \frac{1}{2}[1 - D(\rho_0, \rho_1)], \tag{4}$$

where $D(\rho_0, \rho_1)$ is the trace distance [1,2,33] between the two density matrices ρ_0 and ρ_1 defined as

$$D(\rho_0, \rho_1) = \frac{1}{2} \text{tr}[|\rho_0 - \rho_1|] = \frac{1}{2} \sum_{j=1}^{N} |\lambda_j|. \tag{5}$$

Here $\text{tr}[|A|]$ is known as the "trace norm" with $|A| = \sqrt{A^\dagger A}$, where $A = \rho_0 - \rho_1$, which has the corresponding eigenvalues λ_j. The distance measure given here ranges in value from 0, where the two states are identical, to 1, where the two states are orthogonal, while the corresponding probability of error ranges from 1/2 to 0, respectively. Also the relation in Eq. (4) applies equally to pure or mixed quantum states. For more on

the benefits and properties of the trace distance, see, e.g., the discussion in [34]. Finally, we point out that in the case of distinguishing between two pure states we have the relation between the trace distance and the fidelity F given by $D(\rho_0, \rho_1) = \sqrt{1 - F}$ [32,34]. In the case of two pure coherent states $|\alpha\rangle$ and $|\beta\rangle$ the probability of error can be written as

$$p_e = \frac{1}{2}(1 - \sqrt{1 - |\langle \beta | \alpha \rangle|^2}) \tag{6}$$

and is known as the Helstrom bound [2].

III. DISTINGUISHING PURE AND MIXED COHERENT STATES

We will now consider distinguishing between two pure and mixed coherent states using the previously defined probability of error. A coherent state is defined as $|\alpha\rangle = D(\alpha)|0\rangle$, where $D(\alpha) = \exp(\alpha \hat{a}^\dagger - \alpha^* \hat{a})$ is the displacement operator and can be written in terms of the Fock state basis as

$$|\alpha\rangle = \exp\left(-\frac{1}{2}|\alpha|^2\right) \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle. \tag{7}$$

A coherent state is also a minimum uncertainty state as well as an eigenstate of the annihilation operator $\hat{a}$, i.e., $\hat{a}|\alpha\rangle = \alpha|\alpha\rangle$, where $\alpha = x + ip$ is the amplitude of the electromagnetic wave with $\hbar = 1/2$. Any two coherent states $|\alpha\rangle$ and $|\beta\rangle$ are always nonorthogonal and only approach orthogonality (i.e., $\langle \alpha | \beta \rangle \to 0$) when $|\alpha - \beta| \gg 1$, where the magnitude is $|\langle \alpha | \beta \rangle|^2 = \exp(-|\alpha - \beta|^2)$. For more background on this, see, e.g., [35]. In the following analysis we will define a coherent state displaced in the amplitude and phase quadratures by an amount x and p, respectively, as

$$|\alpha\rangle \equiv |x + ip\rangle. \tag{8}$$

Consequently, we can write the density operators of two pure coherent states ρ_{p0} and ρ_{p1} that we will consider here as

$$\rho_{p0} = |x + ip\rangle\langle x + ip|,$$

$$\rho_{p1} = |-x + ip\rangle\langle -x + ip|. \tag{9}$$

(Note that in this paper we will interchangeably use the words "operator" and "matrix.") In our analysis we also consider two mixed coherent states, where each mixed state is an incoherent mixture of two pure coherent states with equal and opposite displacements in the phase quadrature. The density operators corresponding to these two mixed states, ρ_{m0} and ρ_{m1}, are defined as

$$\rho_{m0} = \frac{1}{2}(|x + ip\rangle\langle x + ip| + |x - ip\rangle\langle x - ip|),$$

$$\rho_{m1} = \frac{1}{2}|-x + ip\rangle\langle -x + ip| + |-x - ip\rangle\langle -x - ip|). \tag{10}$$

Figures 1(a) and 1(b) give a two-dimensional (2D) phase-space illustration of the two pure coherent and the two mixed coherent states as defined by Eqs. (9) and (10), respectively. While Fig. 2 gives an outline of the type of distinguishability situation, we consider different values of x and p.

According to Eq. (5) we need to determine the eigenvalues of $A = \rho_0 - \rho_1$ for both the two pure $A^{(p)}$ and the two
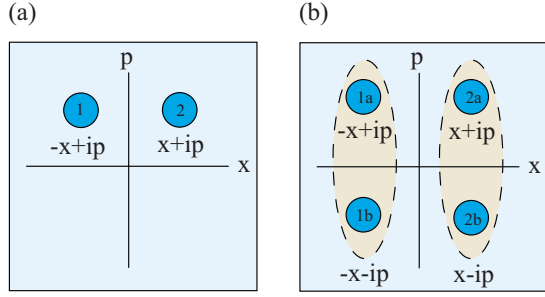
(a)　　　　　　　(b)

FIG. 1. (Color online) Phase-space representation of (a) two pure coherent states (described by the density operators ρ_{p_1} and ρ_{p_0}) and (b) two mixed coherent states (ρ_{m_1} and ρ_{m_0}) for various values of position x and momentum p. Here the dotted lines and shadings in (b) indicate which of the two coherent states are mixed.

mixed $A^{(m)}$ states, in order to eventually calculate the probability of error. To do this we write A in its matrix representation which can be expanded in terms of the Fock state $|n\rangle$ basis defined as [35]

$$|n\rangle = \frac{(\hat{a}^{\dagger})^n}{\sqrt{n!}}|0\rangle, \qquad (11)$$

where $\hat{a}^{\dagger}$ is the creation operator of a quantum harmonic oscillator with $n \in [0, \infty)$. For example, the coherent state $|x+ip\rangle$ can be written in terms of the Fock state basis using Eq. (7) as follows:

$$|x+ip\rangle = e^{-|x+ip|^2/2} \sum_{n=0}^{\infty} \frac{(x+ip)^n}{\sqrt{n!}}|n\rangle. \qquad (12)$$

Once A is written in matrix form we can then numerically determine its eigenvalues up to certain values of n. First though we want to see what form the matrix elements take. Hence, in this Fock state expansion, the inner product of an arbitrary coherent state with a Fock state is given by

$$\langle n | \pm x \pm ip \rangle = \frac{(\pm x \pm ip)^n}{\sqrt{n!}} \exp\left(-\frac{1}{2}(x^2 + p^2)\right), \quad (13)$$

$$\langle \pm x \pm ip | m \rangle = \frac{(\pm x \mp ip)^m}{\sqrt{m!}} \exp\left(-\frac{1}{2}(x^2 + p^2)\right), \quad (14)$$
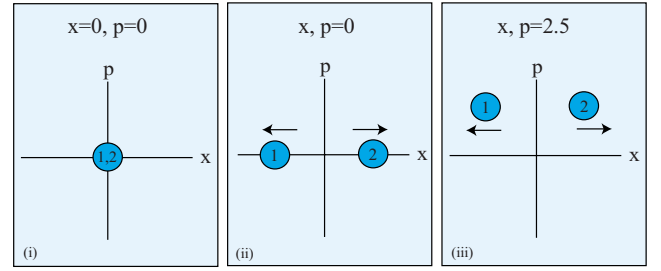
where $|n\rangle$ and $|m\rangle$ are Fock states. Calculating the general matrix coefficients for the case of two pure coherent states, we obtain

$$\langle n | A^{(p)} | m \rangle = \frac{\exp(-x^2 - p^2)}{\sqrt{n!\, m!}} [(x+ip)^n (x-ip)^m$$
$$- (-x+ip)^n (-x-ip)^m]. \qquad (15)$$

Similarly for the two mixed state cases we find

$$\langle n | A^{(m)} | m \rangle = \frac{\exp(-x^2 - p^2)}{2\sqrt{n!\, m!}} [(x+ip)^n (x-ip)^m$$
$$+ (x-ip)^n (x+ip)^m - (-x+ip)^n (-x-ip)^m$$
$$- (-x-ip)^n (-x+ip)^m]. \qquad (16)$$

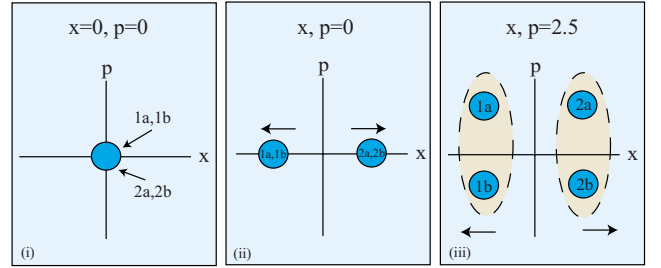(a) Pure coherent states

(b) Mixed coherent states

FIG. 2. (Color online) Examples of the type of distinguishability situations we consider in this paper. Due to the way that we have set up our phase-space configurations (c.f. Fig. 1) we keep the momentum fixed and vary the position in both the pure and the mixed state cases. For example, in the pure state case (a)(i) when $x=p=0$ the two pure states overlap completely and are therefore indistinguishable. (a)(ii) We then keep p fixed and move the pure states further apart by varying x. (a)(iii) This is then repeated for other fixed values of p. A similar situation is considered for the mixed state case (b). Here when $p=0$ [(b)(i),(b)(ii)] we recover the pure state case, while for $p \neq 0$, we have the distinguishability of two mixed coherent states (b)(iii).

Numerically we can calculate the eigenvalues of Eqs. (15) and (16) up to certain values of n and m. Then according to Eq. (4) this will give us the probability of error in distinguishing between two quantum states. These probabilities of errors are plotted in Fig. 3 for the pure and the mixed state cases using $n=m=50$. Our choice of $n=m=50$ is based on the fact that it gives a good approximation (resolution) given our choice of axis values (i.e., $0 \leq x, p \leq 2.5$). For example, consider the various limits of our Fock state expansion. When $n=m=0$ we have an error probability independent of the value of x and p. This is because we are essentially distinguishing between two vacuum states and hence $p_e = 1/2 \ \forall x, p$. At the other limit when $n=m \to \infty$ we have an "ideal" coherent state and, therefore, the resolution of our plot of p_e is perfect for any values of x and p. Accordingly, anywhere in between these limits the value of n and m is dependent on the scaling of x and p. Thus, by using $n=m=50$ we get a good approximation of p_e when $0 \leq x, p \leq 2.5$.

From Fig. 3 we can see that both follow the same overall pattern: for various fixed values of momentum p, position x starts from a probability of error of $p_e = 0.5$ when there is no displacement (indistinguishable and hence 50% chance of guessing the right bit) and tends to $p_e = 0$ after a certain position value $x \approx 1.5$ (this value of x was obtained numeri-
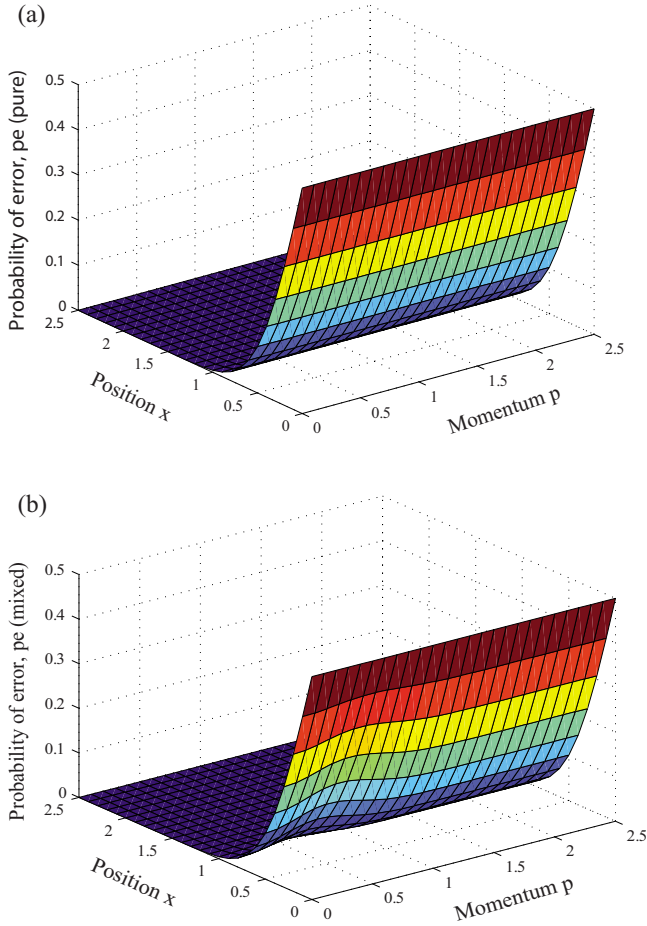
(a)

(b)

FIG. 3. (Color online) Individual plots of the probability of error for (a) two pure coherent states and (b) two mixed coherent states using $n=m=50$. Here our values for both position and momentum start at 0 and go to 2.5. Both plots exhibit the same overall behavior where the probability of error for the pure state case is independent of the momentum value while, for the mixed state case, the probability of error is dependent on certain values of the momentum: $\approx 0 \leq p \leq 1.5$, which alters the probability of error.

cally). We note that a difference between the pure and the mixed state cases is the role of p. In the pure state case, as expected, the probability of error is the same for any value of p when x is varied. However, there is a small region in the mixed state case $\approx 0 \leq p \leq 1.5$, where for these different values of p the probability of error changes. More specifically, in this region the mixed state probability of error is greater than the pure state probability of error,

$$p_e^{(m)} > p_e^{(p)}. \tag{17}$$

After $\approx p > 1.5$ the two become approximately equal. As we will see, this is what results in the difference in information rates (for certain values of x and p) between the pure and the mixed coherent states. Now having numerically calculated p_e, we would like to interpret this in terms of the information gained from using the distinguishing measure, i.e., the probability of error.
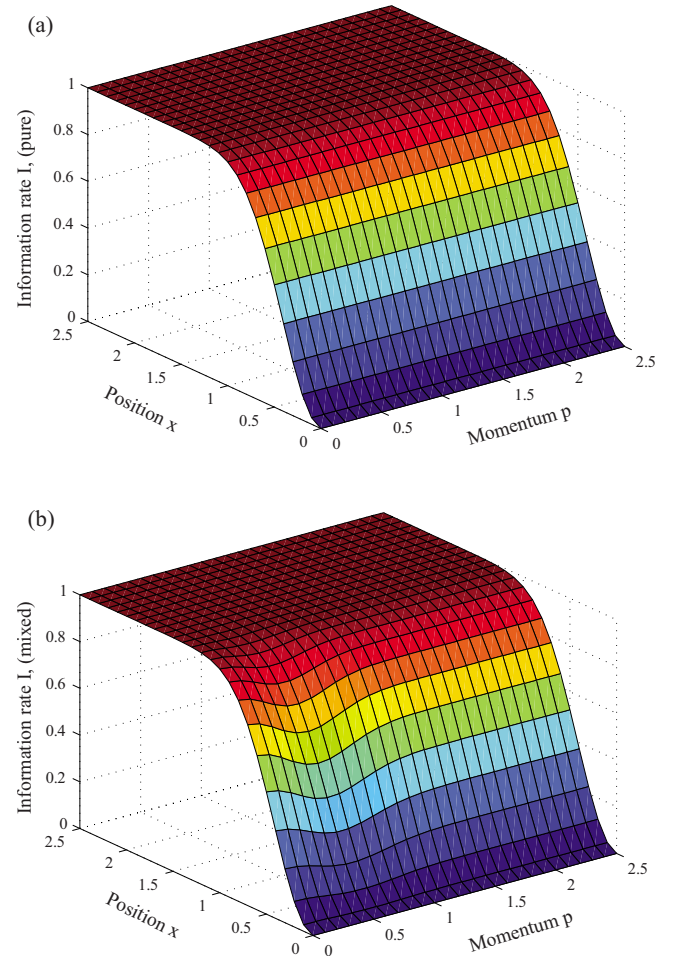
(a)

(b)

FIG. 4. (Color online) Individual plots of the information rate for (a) two pure coherent states and (b) two mixed coherent states. Again we have expanded up to $n=m=50$ Fock states in our analysis.

A. Shannon information

The information obtained by distinguishing between two states can be calculated using the well-known Shannon information formula for a binary symmetric channel [36],

$$I = 1 + p_e \log_2 p_e + (1 - p_e)\log_2(1 - p_e). \tag{18}$$

Figure 5 shows the difference between the Shannon information obtained by distinguishing between two coherent states $I(\rho_{p_0}, \rho_{p_1})$ compared with distinguishing between two mixed coherent states $I(\rho_{m_0}, \rho_{m_1})$ (where the individual cases are plotted in Fig. 4). This information difference is defined as the information gain I_{gain},

$$I_{gain} = I(\rho_{p_0}, \rho_{p_1}) - I(\rho_{m_0}, \rho_{m_1}). \tag{19}$$

Figure 5 plots I_{gain} in terms of the position (amplitude) and momentum (phase) quadrature displacements of the pure and the mixed states as defined in Eqs. (9) and (10), respectively. Here we have expanded up to 50 Fock states, i.e., $n=m=50$ in our numerical analysis.

There are two main features of Fig. 5. First, we notice that, given our distinguishability measure and initial configu-
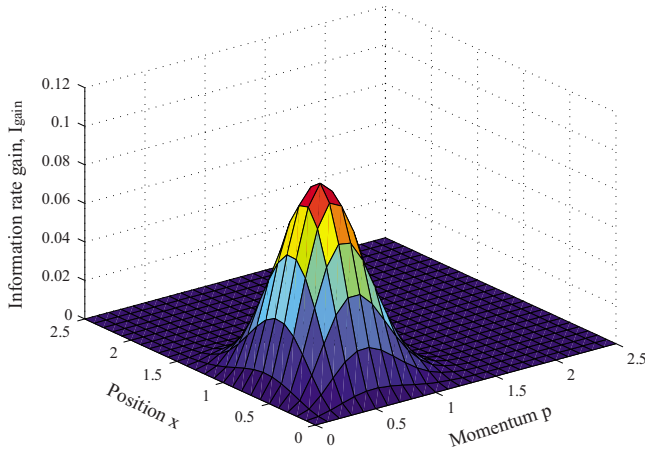
FIG. 5. (Color online) The difference in information rates between two pure coherent and two mixed coherent states in terms of the position (amplitude) and momentum (phase) quadratures. Here $I_{gain}=I(\rho_{p_0},\rho_{p_1})-I(\rho_{m_0},\rho_{m_1})$. For the particular distinguishability case consider here, the two mixed states never give more information than two pure states, which allows us to upper bound information rates in CV-QKD using the postselection protocol.

ration of coherent states in phase space, two mixed states never give more information than two pure states, i.e.,

$$I(\rho_{m0},\rho_{m1}) \leq I(\rho_{p0},\rho_{p1}). \tag{20}$$

This result is relevant given that in the original postselection CV-QKD protocol [26] it means that an eavesdropper is upper bounded, in terms of her accessible information, when choosing to distinguish between two pure coherent states (instead of the two mixed coherent states). Second, there is a flat region where the information gain is zero, i.e., $I_{gain}=0$, where the information from distinguishing between two mixed states is the same as that of two pure states. This means that as the pure coherent and the mixed coherent states are moved further and further apart in the amplitude quadrature (for fixed values of momentum), the probability of error tends to the same value (i.e., $p_e=0$) and hence the same amount of information is obtained from both (c.f. Fig. 3). So in some sense, at a certain point the two mixed states start behaving (from a distinguishability point of view) like two pure states. This only starts occurring for the mixed states when the value of p is greater than a particular value. This is because we require that the individual mixed states themselves are further apart (in p value) and hence more distinguishable individually, before we can then start distinguishing each of the two mixed states with one other.

1. Discussion: Maximum accessible information for an eavesdropper

We now briefly note the equivalence between the information rate obtained using the probability of error as defined in Eq. (4) and the Levitin information bound [38] which is used in postselection CV-QKD to ascertain how much information an eavesdropper gains. The original postselection protocol [26] involves the generation of a secure key by Alice sending Bob coherent states that have had classical vari-

ables $\{x,p\}$ encoded on them. Bob measures these states using homodyne (or heterodyne [30]) detection and then decodes them using some previously agreed upon binary encoding. To calculate how much information an eavesdropper can optimally obtain during the protocol, we use the Levitin bound [38] which determines the maximum accessible information from distinguishing between two nonorthogonal pure states, i.e.,

$$I_{AE} = \tfrac{1}{2}(1 + \sqrt{1 - |z|^2})\log_2(1 + \sqrt{1 - |z|^2})$$
$$+ \tfrac{1}{2}(1 - \sqrt{1 - |z|^2})\log_2(1 - \sqrt{1 - |z|^2}), \tag{21}$$

where I_{AE} denotes the mutual information between Alice and the eavesdropper, Eve. Here z is the overlap of the two pure coherent states which Eve needs to distinguish between, i.e., $z=\langle -x+ip|x+ip\rangle=\exp[-2(x^2+ixp)]$ [35], where the modulus squared is the Gaussian $|z|^2=\exp(-4x^2)$. Again we assumed that the channel transmission is set to unity. We note here that Eq. (21) can be alternately derived by simply using the probability of error given by the Helstrom bound for two pure coherent states, i.e., Eq. (6), and substituting that into Shannon's formula given in Eq. (18). Consequently, after some simple algebra, we see that $I(\rho_{p0},\rho_{p1})=I_{AE}$. This result only applies to the pure state case. The question of maximizing the accessible information in CV quantum state discrimination (and hence, in CV-QKD eavesdropping analysis) for two general mixed quantum states is still an open question, although Levitin does discuss a specific (nongeneral) situation in [38].

B. Homodyne detection versus POVM: Pure and mixed state cases

In this section we consider the following questions: what is the probability of error in distinguishing between two pure coherent and two mixed coherent states (whose orientation is defined in Fig. 1) given that a homodyne detection (also known as a projective or von Neumann) measurement is performed? And how does that compare to the probability of error defined using the trace distance? Homodyne detection is one of the most commonly used methods of measurement in CV quantum communication protocols [3] and, consequently, these questions are of practical interest, particularly for CV-QKD. We note that previous work on this includes binary optical communication distinguishability using direct and homodyne detection in realistic situations [11], as well as optical pure coherent state distinguishability which has been theoretically [16–21] and experimentally investigated [22,23]. However, in the following analysis we consider a specific distinguishability situation for both the pure and the mixed coherent state cases as given in Fig. 1, which is motivated by postselection CV-QKD.

We will first analyze the pure state case as the results for both the pure state and the mixed state cases will be the same. The reason for this can be seen from Fig. 1 where an $\hat{x}$ quadrature measurement will collapse and project the mixed states onto the x axis in the same way as the pure state case does. An $\hat{x}$ quadrature measurement using homodyne detection is modeled theoretically by acting a projective measure-

ment $|x\rangle\langle x|$ on the two pure coherent states $|x+ip\rangle$ and $|-x+ip\rangle$. The probability of obtaining the measurement outcome m is given by [11,37]

$$P(m||\pm x+ip\rangle) = |\langle x|\pm x+ip\rangle|^2 = \sqrt{\frac{2}{\pi}}e^{-2(m\mp x)^2}. \quad (22)$$

Such a formula is used to derive information rates for (the receiver) Bob in the CV-QKD postselection protocol; except in the above formula the loss on the quantum channel η (which is typically associated with the eavesdropper) is set to unity $\eta=1$. The probability of error $p_e^{(p)}$, when a projective measurement is performed to distinguish between the two pure coherent states, can now be written as

$$p_e^{(p)} = \begin{cases} \dfrac{P(m||-x+ip\rangle)}{P(m||x+ip\rangle) + P(m||-x+ip\rangle)} & \text{for } m > 0 \\[4mm] \dfrac{P(m||x+ip\rangle)}{P(m||x+ip\rangle) + P(m||-x+ip\rangle)} & \text{for } m < 0. \end{cases}$$

$$(23)$$

Substituting Eq. (22) into Eq. (23) leads to

$$p_e^{(p)} = \begin{cases} \dfrac{e^{-2(m+x)^2}}{e^{-2(m-x)^2} + e^{-2(m+x)^2}} & \text{for } m > 0 \\[4mm] \dfrac{e^{-2(m-x)^2}}{e^{-2(m-x)^2} + e^{-2(m+x)^2}} & \text{for } m < 0. \end{cases} \quad (24)$$

The final probability of error $\bar{p}_e^{(p)}$ once we have integrated over all possible measurement results m is given by

$$\bar{p}_e^{(p)} = 2\int_0^\infty dm\, p_e^{(p)} P(m||x+ip\rangle)$$

$$= \sqrt{\frac{8}{\pi}} \int_0^\infty \frac{dm}{e^{2(m+x)^2} + e^{2(-m+x)^2}}. \quad (25)$$

We numerically evaluate the above integral and plot the results in Fig. 6(a). Again the resulting plots for both the pure and the mixed state cases are identical. Figure 6(a) has similar behavior as that of the probability of error obtained using the trace distance for the pure coherent state case, i.e., Fig. 3(a). Because the probability of errors given in Figs. 3(a) and 6(a) are independent of the value of momentum, we can plot a 2D cross-sectional slice of the probability of error for both the POVM and the projective measurement cases. This is given in Fig. 6(b) where it can be seen that the measurement associated with the probability of error using a POVM (i.e., as a function of the trace distance) is lower than the projective $\hat{x}$ quadrature homodyne detection measurement. The distance between the two outside curves in Fig. 6(b) is slightly reduced for certain values of p when considering the mixed state case. For example, in Fig. 3(b) for values where $0 < p \leq 1.5$ the probability of error is slightly increased. We illustrate this in Fig. 6(b) by plotting the mixed state case for $p = 0.55$.
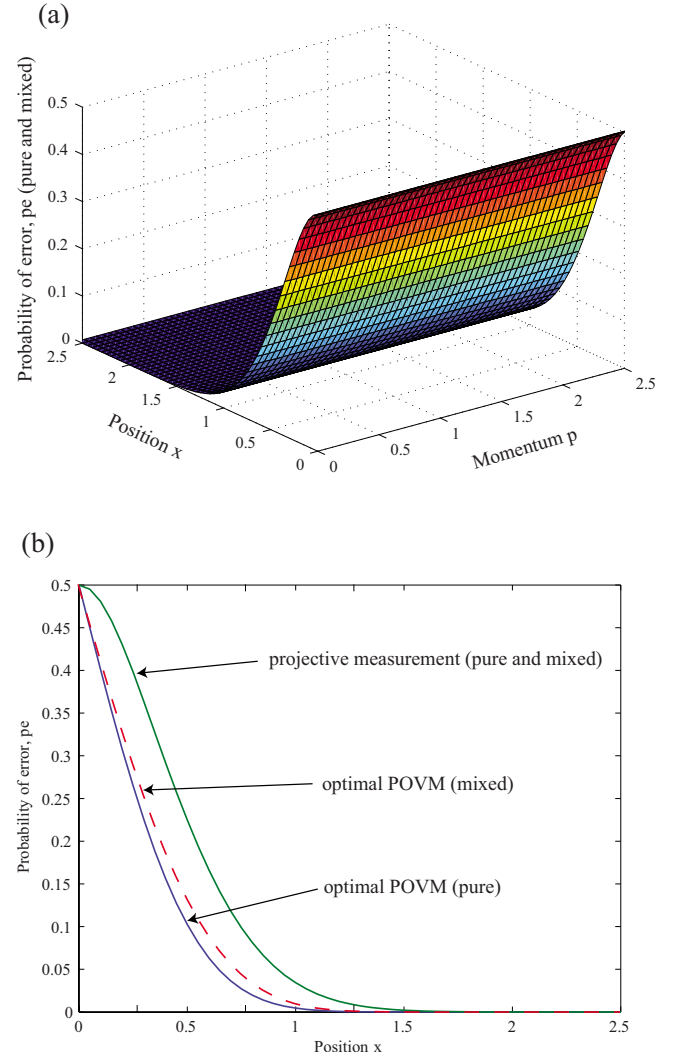

FIG. 6. (Color online) Probability of error plots for the coherent state analysis. (a) The plot of the probability of error for both the pure and the mixed coherent states for an x quadrature measurement. Both are identical due to the fact that now a projective (homodyne) measurement is performed on each of the quantum states rather than the usual POVM as considered before. (b) Optimal POVMs versus projective measurements for the pure and the mixed coherent state cases. In Fig. 3(a) and (a), due to probability of error being independent of the momentum variable p, we can take a cross-sectional slice at any value of p and plot the probability of error as a function of x for both types of measurements. We also plot a cross-sectional slice from the mixed state case given in Fig. 3(b) for $p = 0.55$ (red dashed line). As expected the POVM minimizes the probability of error, i.e., the projective measurement is not the optimal type of distinguishability measurement.

IV. DISTINGUISHING PURE AND MIXED SQUEEZED STATES

Having analyzed the distinguishability of pure and mixed coherent states, we now extend our analysis to another set of Gaussian states: squeezed states. Figure 7 gives a phase-space representation of the distinguishability situation we consider, i.e., it is the same configuration as the coherent state case except now we are considering it for displaced
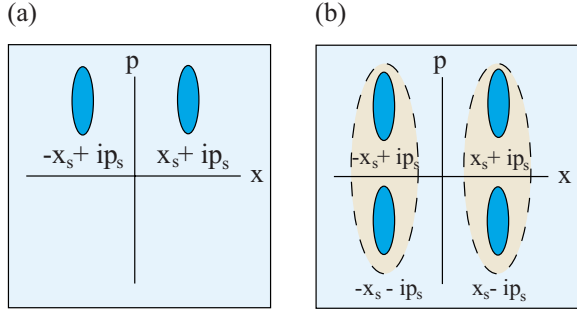
FIG. 7. (Color online) Phase-space representation of (a) two pure squeezed states (described by the density operators ρ_{p_1} and ρ_{p_0}) and (b) two mixed squeezed states (ρ_{m_1} and ρ_{m_0}) for arbitrary displacements $\{x_s, p_s\}$. Again, just as with the coherent state configuration, the dotted lines and shadings in (b) indicate which of the two squeezed states form a mixture.

squeezed states. A displaced squeezed vacuum state [35] is defined as

$$|\alpha, \xi\rangle = D(\alpha)S(\xi)|0\rangle, \quad (26)$$

where $S(\xi)$ is the single-mode squeezed gate defined as

$$S(\xi) = \exp[\xi(\hat{a}^2 - \hat{a}^{\dagger 2})/2] = \exp[i\xi(\hat{x}\hat{p} + \hat{p}\hat{x})] \quad (27)$$

with $\xi = r\exp(i\theta)$. Here r is known as the squeezing parameter ($r \in [0, \infty)$) performed (in our case) in only one (position) quadrature direction and $0 \le \theta \le 2\pi$ with $D(\alpha)$ again being the displacement gate. As can be seen, the above state is created by first squeezing the vacuum state $|0\rangle$ and then displacing it. We will now define the density operators of two pure squeezed states that we consider as

$$\rho_{p0} = |x_s + ip_s\rangle\langle x_s + ip_s|, \quad (28)$$

$$\rho_{p1} = |-x_s + ip_s\rangle\langle -x_s + ip_s|, \quad (29)$$

where the subscript s indicates that we are now considering the squeezed state situation. We can define the density operators of two arbitrary mixed squeezed states ρ_{m0} and ρ_{m1} as

$$\rho_{m0} = \frac{1}{2}(|x_s + ip_s\rangle\langle x_s + ip_s| + |x_s - ip_s\rangle\langle x_s - ip_s|), \quad (30)$$

$$\rho_{m1} = \frac{1}{2}(|-x_s + ip_s\rangle\langle -x_s + ip_s| + |-x_s - ip_s\rangle\langle -x_s - ip_s|). \quad (31)$$

As with the coherent state analysis, we need to ultimately determine the eigenvalues of the appropriate matrices in order to calculate the trace distance and then the probability of error. Again this involves expanding the matrix in an orthogonal basis, i.e., the Fock state basis. With this in mind, a displaced squeezed state can be expanded in terms of Fock states as [35]

$$|\alpha, \xi\rangle = \frac{1}{\sqrt{\cosh r}}\exp\left[-\frac{1}{2}(|\alpha|^2 + \alpha^{*2}e^{i\theta}\tanh r)\right]$$
$$\times \sum_{n=0}^{\infty} \frac{\left[\frac{1}{2}e^{i\theta}\tanh r\right]^{n/2}}{\sqrt{n!}} H_n[\gamma(e^{i\theta}\sinh 2r)^{-1/2}]|n\rangle, \quad (32)$$

where $\alpha = x_s + ip_s$ and $\gamma = \alpha\cosh r + \alpha^* e^{i\theta}\sinh r$. Here $H_n(x)$ are the Hermite polynomials of degree n which are a polynomial sequence defined as

$$H_n(x) = (-1)^n e^{x^2}\frac{d^n}{dx^n}e^{-x^2}, \quad (33)$$

where in our case $x \equiv \gamma(e^{i\theta}\sinh 2r)^{-1/2}$. We point out that in the limit $r \to 0$ in Eq. (32) we simply get back the coherent state as given by Eq. (7). Note that in our calculations we will only consider the case when $\theta = 0$, i.e., the squeezed states are only squeezed along the position quadrature (c.f. Fig. 7) and not at some angle θ.

Using Eq. (32) the overlap of a Fock state and a displaced squeezed state is given by

$$\langle n|\alpha, \xi\rangle = (n!\ \cosh r)^{-1/2}\exp\left[-\frac{1}{2}(|\alpha|^2 + \alpha^{*2}e^{i\theta}\tanh r)\right]$$
$$\times\left[\frac{1}{2}e^{i\theta}\tanh r\right]^{n/2}H_n[\gamma(e^{i\theta}\sinh 2r)^{-1/2}]. \quad (34)$$

We also have for the other matrix elements

$$\langle \alpha, \xi|m\rangle = (m!\ \cosh r)^{-1/2}\exp\left[-\frac{1}{2}(|\alpha|^2 + \alpha^2 e^{-i\theta}\tanh r)\right]$$
$$\times\left[\frac{1}{2}e^{-i\theta}\tanh r\right]^{m/2}H_m[\gamma^*(e^{-i\theta}\sinh 2r)^{-1/2}]. \quad (35)$$

Writing the above in the x and p notation gives us

$$\langle n|x_s + ip_s\rangle = (n!\ \cosh r)^{-1/2}$$
$$\times\exp\left\{-\frac{1}{2}[x_s^2 + p_s^2 + (x_s - ip_s)^2 e^{i\theta}\tanh r]\right\}$$
$$\times\left[\frac{1}{2}e^{i\theta}\tanh r\right]^{n/2}H_n[\gamma(e^{i\theta}\sinh 2r)^{-1/2}], \quad (36)$$

where $\gamma = (x_s + ip_s)\cosh r + (x_s - ip_s)e^{i\theta}\sinh r$. We also have

$$\langle x_s + ip_s|m\rangle = (m!\ \cosh r)^{-1/2}$$
$$\times\exp\left\{-\frac{1}{2}[x_s^2 + p_s^2 + (x_s + ip_s)^2 e^{-i\theta}\tanh r]\right\}$$
$$\times\left[\frac{1}{2}e^{-i\theta}\tanh r\right]^{m/2}H_m[\gamma^*(e^{-i\theta}\sinh 2r)^{-1/2}] \quad (37)$$

with $\gamma^* = (x_s - ip_s)\cosh r + (x_s + ip_s)e^{-i\theta}\sinh r$. Again calculating the general matrix coefficients for the case of the two pure squeezed states we obtain

$$\langle n|A_s^{(p)}|m\rangle = \frac{(n!\ m!)^{-1/2}}{\cosh r}\left(\frac{1}{2}\tanh r\right)^{(n+m)/2}$$
$$\times\exp\{-[x_s^2 + p_s^2 + \tanh r(x_s^2 - p_s^2)]\}$$
$$\times[H_n(\gamma)H_m(\gamma^*) - H_n(\gamma')H_m(\gamma^{*\prime})], \quad (38)$$

where $A_s^{(p)} = \rho_{p0} - \rho_{p1}$ and $\theta = 0$. Here the Hermite polynomials are defined as

$$H_n(\gamma) \equiv H_n[\gamma(\sinh 2r)^{-1/2}],$$

$$H_m(\gamma^*) \equiv H_m[\gamma^*(\sinh 2r)^{-1/2}],$$

$$H_n(\gamma') \equiv H_n[\gamma'(\sinh 2r)^{-1/2}],$$

$$H_m(\gamma'^*) \equiv H_m[\gamma'^*(\sinh 2r)^{-1/2}], \quad (39)$$

where γ is defined as usual (but now with $\theta=0$) and $\gamma'=(-x_s+ip_s)\cosh r+(-x_s-ip_s)\sinh r$. Similarly for the two mixed squeezed states we find that the matrix elements are given by

$$\langle n|A_s^{(m)}|m\rangle = \frac{1}{2}\frac{(n!\,m!)^{-1/2}}{\cosh r}\left(\frac{1}{2}\tanh r\right)^{(n+m)/2}$$
$$\times\exp\{-[x_s^2+p_s^2+(x_s^2-p_s^2)\tanh r]\}$$
$$\times[H_n(\gamma)H_m(\gamma^*)+H_n(\gamma')H_m(\gamma'^*)$$
$$-H_n(\gamma')H_m(\gamma'^*)-H_n(\gamma'')H_m(\gamma''^*)], \quad (40)$$

where $A_s^{(m)}=\rho_{m0}-\rho_{m1}$ and the Hermite polynomials are defined previously in Eq. (39) with the new additional variables

$$\gamma'' = (x_s-ip_s)\cosh r+(x_s+ip_s)\sinh r, \quad (41)$$

$$\gamma''' = (-x_s-ip_s)\cosh r+(-x_s+ip_s)\sinh r \quad (42)$$

plus their respective conjugates. We can simplify the Hermite polynomials in Eq. (40) by realizing that the following relations hold:

$$\gamma'' = \gamma^*, \quad \gamma''' = \gamma'^* \quad (43)$$

plus their conjugates. Therefore Eq. (40) can be rewritten as

$$\langle n|A_s^{(m)}|m\rangle = \frac{1}{2}\frac{(n!\,m!)^{-1/2}}{\cosh r}\left(\frac{1}{2}\tanh r\right)^{(n+m)/2}$$
$$\times\exp\{-[x_s^2+p_s^2+(x_s^2-p_s^2)\tanh r]\}$$
$$\times[H_n(\gamma)H_m(\gamma^*)+H_n(\gamma^*)H_m(\gamma)$$
$$-H_n(\gamma')H_m(\gamma'^*)-H_n(\gamma'^*)H_m(\gamma')]. \quad (44)$$

Numerically we can calculate the eigenvalues of Eqs. (38) and (44) for two values of the squeezing parameter r. According to Eq. (4) this will give us the probability of error in distinguishing between the two sets of quantum states. Our results are plotted in Figs. 8(a), 8(c), 8(e), and 8(g) where we have set $\theta=0$ and used two squeezing parameters: (1) $r=0.35$ which corresponds to approximately 3 dB of squeezing and (2) $r=0.7$ (6 dB) [these conversions are obtained by using the formula $-10\log_{10}(e^{-2r})$ dB]. We can see that as the squeezing is increased the probability of error is reduced in both the pure and the mixed state cases. For example, in the coherent state case for fixed values of momentum $p_e \to 0$ when $\approx x\geq 1.5$. However, in the pure squeezed state case, we numerically find that the position value is $\approx x \geq 1.1$ for 3 dB of squeezing and $\approx x\geq 0.8$ for 6 dB. The reason why this occurs can be seen by comparing the distinguishability of two pure coherent states with two pure squeezed states, if you first picture the two coherent states initially overlapping [at $x=p=0$; c.f. Fig. 2(a)] and then increasing the x distance between them to a point where the phase-space circles no longer overlap. Now doing this again

but with the x quadrature squeezed states, we can see that because these circles are narrower then it takes a smaller distance for them to no longer overlap. Hence, a smaller x is required to achieve a smaller probability of error.

A. Shannon information

Again we calculate the Shannon information to obtain the information rate gain I_{gain} for the two values of squeezing and plot them in Fig. 9 [where the individual rates are given in Figs. 8(b), 8(d), 8(f), and 8(h)]. As with the coherent state analysis, based on our distinguishability measure and initial configuration in phase space, two mixed squeezed states (where each mixed state is an incoherent mixture of two pure squeezed states with equal and opposite displacements in the phase quadrature) never give more information than two pure squeezed states. We again see, after certain values of position and momentum, a flat region in both graphs which indicates that the two mixed states have the same accessible information as the two pure states. This results in a net information rate of $I_{gain}=0$ and is due to the same reason as was given for the coherent states. The effect of increasing the squeezing parameter is given in Figs. 9(a) and 9(b) with a side-on profile depicted in Fig. 9(c). Figure 9(c) shows that by increasing the amount of squeezing in the x direction the effect for fixed p is to narrow the information distribution for different position values. In some sense we have a squeezing of the information rate along the x axis. This comes from the fact that, as mentioned before, as the squeezing increases the probability of error decreases for smaller values of x. This ultimately leads to $I_{gain}\to 0$ for smaller values of x than what we had for the (zero squeezing) coherent state case [c.f. Fig. 9(c)]. Conversely, we also notice that as squeezing is increased, for fixed values of x, the net information rate requires larger values of p until $I_{gain}=0$. This leads to a broadening or an antisqueezing of the information rate along the p direction.

V. DISCUSSION AND CONCLUSION

In our analysis we used the probability of error to discriminate between specific phase-space configurations of two pure and two mixed CV quantum states. Recently, Pirandola and Lloyd [15] combined the Minkowski inequality and the quantum Chernoff bound to derive upper bounds on quantum state discrimination for CV. This was in the context of Gaussian states using symplectic algebraic methods (e.g., see [28]). Future work would entail comparing these techniques to the ones given in this paper and extending it to include other Gaussian states, such as Einstein-Podolsky-Rosen (EPR) states and thermal states.

In conclusion, we have considered a situation in postselection-based CV-QKD where there is an assumption that an eavesdropper upper bounds her information by distinguishing between two pure coherent states instead of distinguishing between two mixed coherent states (where the various mixtures have the same position component). We showed that the eavesdropper will never get more information from the two mixed coherent states. Hence, we have

Pure Squeezed States

(a)

(b)

3 dB Squeezing

(c)

(d)

6 dB Squeezing

Mixed Squeezed States

(e)

(f)
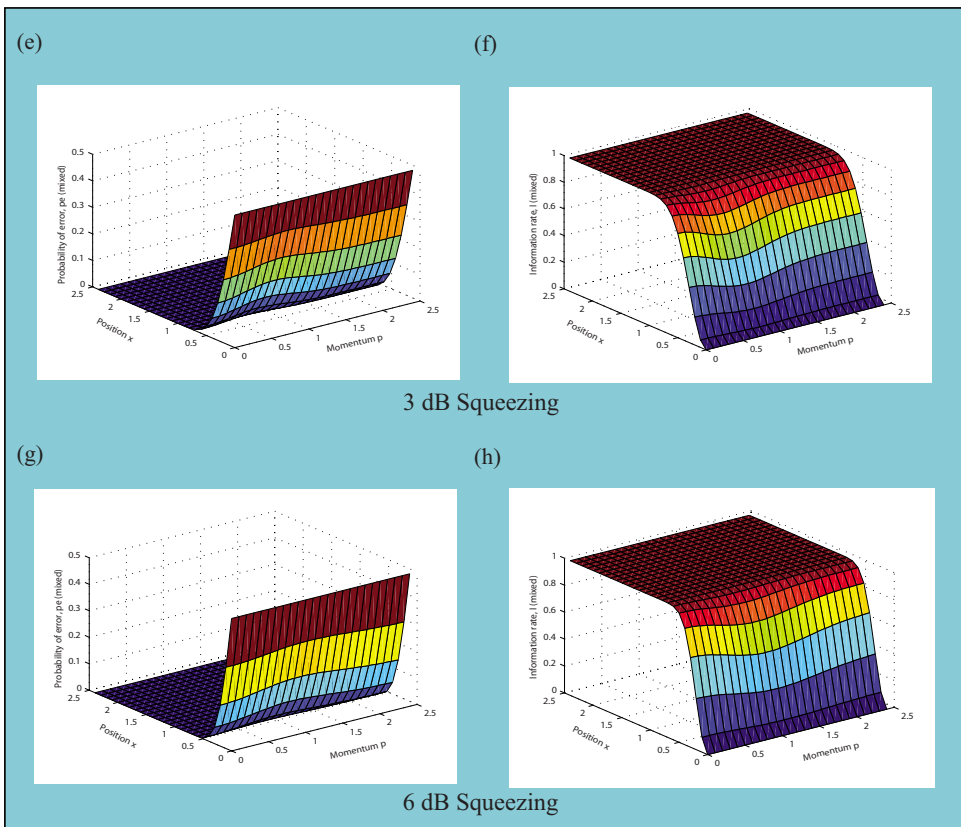
3 dB Squeezing

(g)

(h)
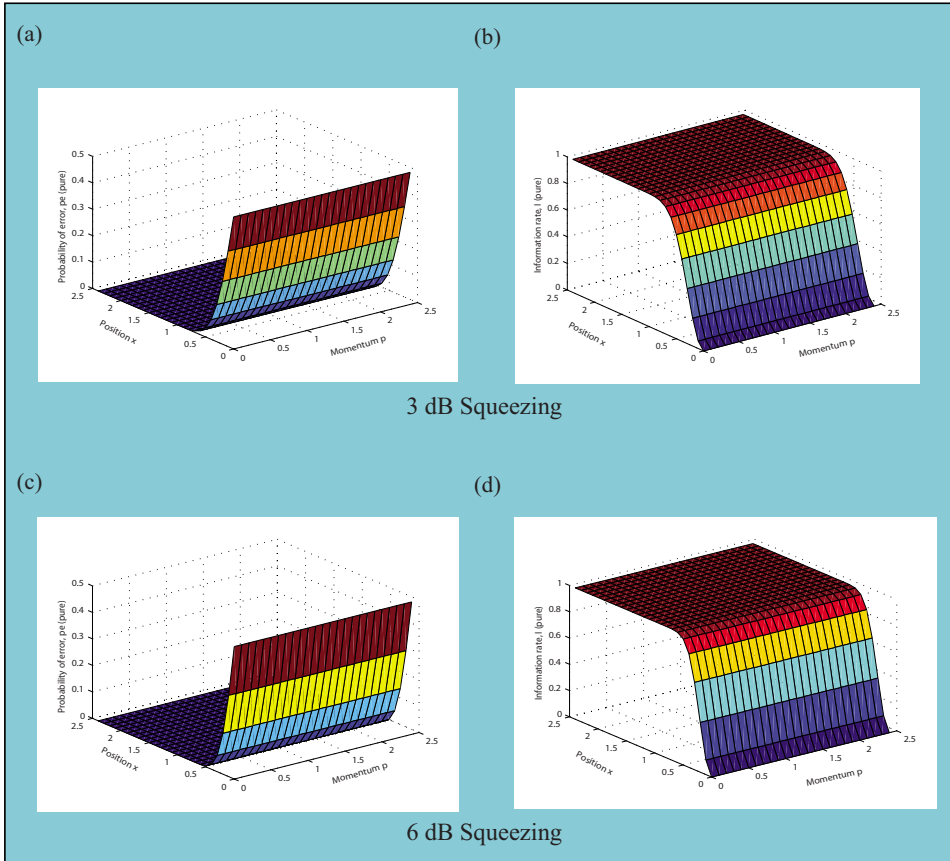
6 dB Squeezing

FIG. 8. (Color online) Individual plots of both the probability of errors and information rates for (a)–(d) two pure squeezed states and (e)–(h) two mixed squeezed states for two types of squeezing parameters: $r=0.35$ (3 dB) and $r=0.70$ (6 dB). These plots reflect the same overall behavior and characteristics of the probability of error and information rates which were exhibited in the coherent state case. The chief difference is the increase in squeezing results in the distinguishability measure p_e tending toward zero for smaller values of position x.
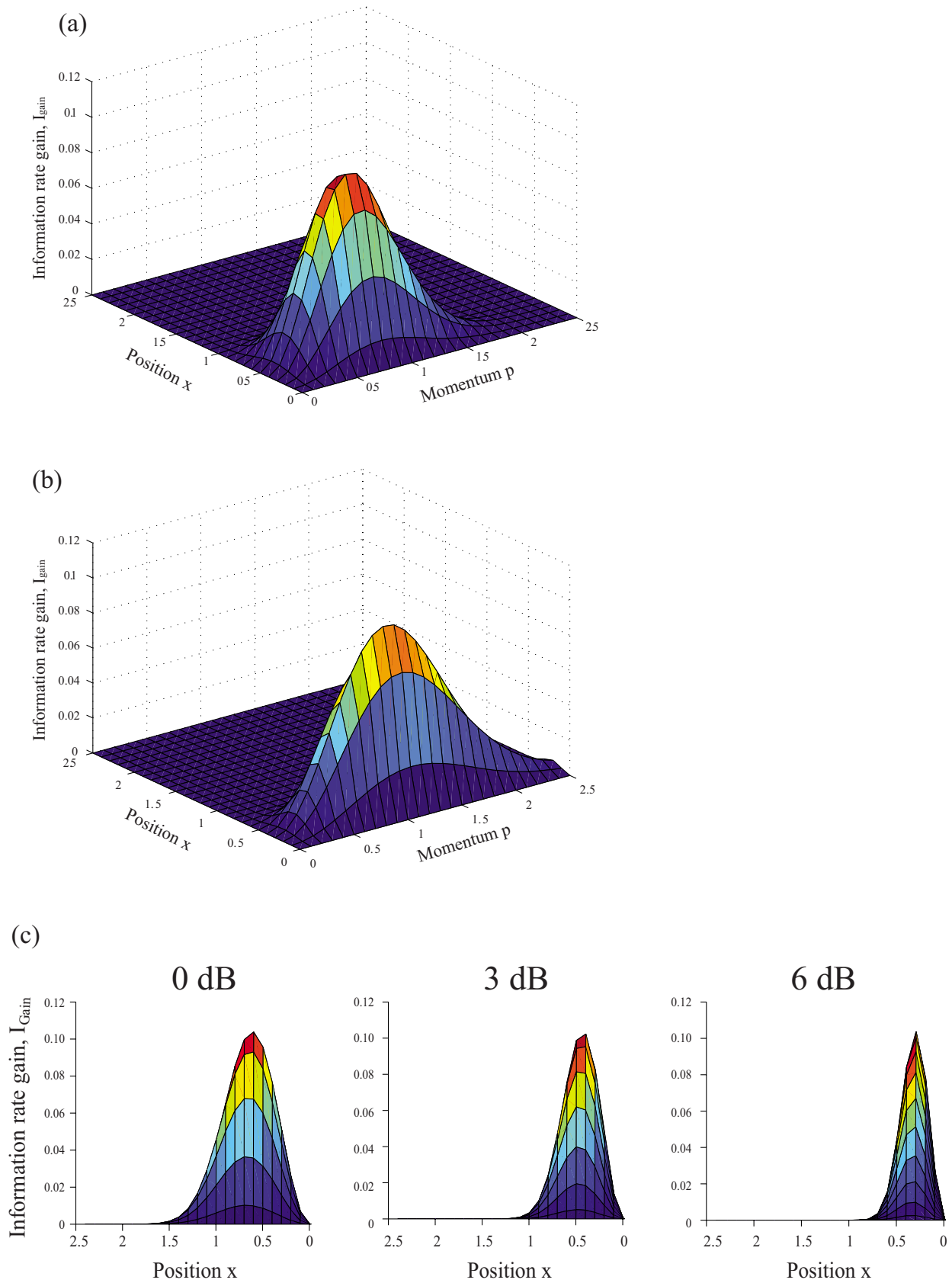
FIG. 9. (Color online) The difference in information rates I_{gain} between the two pure squeezed and two mixed squeezed states for two types of squeezing: (a) $r=0.35$ (3 dB) and (b) $r=0.70$ (6 dB). As with the coherent state case, two mixed squeezed states never give more information than two pure squeezed states, with respect to the phase-space configurations considered in this paper. (c) Side-on profile of the variation in the information distribution for the three cases studied: 0 (coherent state; c.f. Fig. 5), 3, and 6 dB (squeezed states).

proven the assumption to be true. We showed this using the probability of error as the distinguishability measure along with the Shannon information formula. Furthermore, we expanded our analysis to include other types of Gaussian states: pure and mixed squeezed states. In that analysis, the squeezed states are aligned in phase space in the same configuration as were the coherent states. The same types of behavior and characteristics are present in the probability of error and information rate plots for the squeezed states as was for the coherent state case. Furthermore, varying the amount of squeezing results in the squeezing and antisqueezing of the net information gain rates, i.e., smaller values of x and larger values of p are required to reach a net information rate of zero. This corresponds to the case where two mixed squeezed states are as equally likely to be distinguished as two pure squeezed states.

We also considered the practical case where a homodyne detection measurement is used to distinguish the pure and mixed coherent states and compared the probability of error in those situations to the POVM measurement of the trace distance. As expected, we find that the POVM outperforms the projective measurement of the homodyne detector, i.e., it reduces the probability of error.

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).

[2] C. W. Helstrom, *Quantum Detection and Estimation Theory*, Mathematics in Science and Engineering (Academic Press, New York, 1976), Vol. 123.

[3] S. L. Braunstein and P. van Loock, Rev. Mod. Phys. **77**, 513 (2005).

[4] *Quantum Information with Continuous Variables of Atoms and Light*, edited by N. J. Cerf, G. Leuchs, and E. S. Polzik (Imperial College Press, London, 2007).

[5] A. Chefles, Contemp. Phys. **41**, 401 (2000).

[6] J. Bergou, U. Herzog, and M. Hillery, *Discrimination of Quantum States* (Springer-Verlag, New York, 2004).

[7] J. Twamley, J. Phys. A **31**, 3659 (1996).

[8] Gh.-S. Paraoanu and H. Scutaru, Phys. Rev. A **58**, 869 (1998).

[9] A. Chefles and S. M. Barnett, Phys. Lett. A **250**, 223 (1998).

[10] S. J. van Enk, Phys. Rev. A **66**, 042313 (2002).

[11] S. Olivares and M. G. A. Paris, J. Opt. B: Quantum Semiclassical Opt. **6**, 69 (2004).

[12] H. Nha and H. J. Carmichael, Phys. Rev. A **71**, 032336 (2005).

[13] U. L. Andersen, M. Sabuncu, R. Filip, and G. Leuchs, Phys. Rev. Lett. **96**, 020409 (2006).

[14] J. Calsamiglia, R. Munoz-Tapia, L. Masanes, A. Acin, and E. Bagan, Phys. Rev. A **77**, 032311 (2008).

[15] S. Pirandola and S. Lloyd, Phys. Rev. A **78**, 012331 (2008).

[16] S. Dolinar, Research Laboratory of Electronics, MIT, Quarterly Progress Report No. 111, 1973 (unpublished), p. 115.

[17] R. S. Kennedy, Research Laboratory of Electronics, MIT, Quarterly Progress Report No. 108, 1973 (unpublished), p. 219.

[18] M. Takeoka, M. Sasaki, P. van Loock, and N. Lutkenhaus, Phys. Rev. A **71**, 022318 (2005).

[19] M. Sasaki and O. Hirota, Phys. Rev. A **54**, 2728 (1996).

[20] M. Takeoka and M. Sasaki, Phys. Rev. A **78**, 022320 (2008).

[21] J. M. Geremia, Phys. Rev. A **70**, 062303 (2004).

[22] R. L. Cook *et al.*, Nature (London) **446**, 774 (2007).

[23] C. Wittmann, M. Takeoka, K. N. Cassemiro, M. Sasaki, G. Leuchs, and U. L. Andersen, Phys. Rev. Lett. **101**, 210501 (2008).

[24] F. Grosshans, G. Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature (London) **421**, 238 (2003).

[25] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).

[26] C. Silberhorn, T. C. Ralph, N. Lutkenhaus, and G. Leuchs, Phys. Rev. Lett. **89**, 167901 (2002).

[27] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **93**, 170504 (2004).

[28] S. Pirandola, S. Mancini, S. Lloyd, and S. L. Braunstein, Nat. Phys. **4**, 726 (2008).

[29] M. Heid and N. Lutkenhaus, Phys. Rev. A **76**, 022313 (2007).

[30] A. M. Lance, T. Symul, V. Sharma, C. Weedbrook, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **95**, 180503 (2005).

[31] T. Symul, D. J. Alton, S. M. Assad, A. M. Lance, C. Weedbrook, T. C. Ralph, and P. K. Lam, Phys. Rev. A **76**, 030303(R) (2007).

[32] C. A. Fuchs and J. van de Graaf, IEEE Trans. Inf. Theory **45**, 1216 (1999).

[33] M. Reed and B. Simon, *Methods of Modern Mathematical Physics Part I: Functional Analysis* (Academic Press, New York, 1972).

[34] A. Gilchrist, N. K. Langford, and M. A. Nielsen, Phys. Rev. A **71**, 062310 (2005).

[35] C. C. Gerry and P. L. Knight, *Introductory Quantum Optics* (Cambridge University Press, Cambridge, England, 2005).

[36] C. E. Shannon, Bell Syst. Tech. J. **27**, 379 (1948).

[37] U. Leonhardt, *Measuring the Quantum State of Light* (Cambridge University Press, Cambridge, England, 1997).

[38] L. B. Levitin, in *Quantum Communications and Measurement*, edited by V. P. Belavkin, O. Hirota, and R. L. Hudson (Plenum Press, New York, 1995), pp. 439–448.