IOP PUBLISHING JOURNAL OF PHYSICS A: MATHEMATICAL AND THEORETICAL

J. Phys. A: Math. Theor. **42** (2009) 465309 (23pp) doi:10.1088/1751-8113/42/46/465309

Quantum forbidden-interval theorems for stochastic resonance

Mark M Wilde[1,2] **and Bart Kosko**[1]

[1] Center for Quantum Information Science and Technology, Department of Electrical Engineering, University of Southern California, Los Angeles, CA 90089, USA
[2] Hearne Institute for Theoretical Physics, Department of Physics and Astronomy, Louisiana State University, Baton Rouge, LA 70803, USA

E-mail: mark.wilde@alumni.usc.edu

Received 29 April 2009, in final form 19 August 2009
Published 28 October 2009
Online at stacks.iop.org/JPhysA/42/465309

Abstract

We extend the classical forbidden-interval theorems for a stochastic-resonance noise benefit in a nonlinear system to a quantum-optical communication model and a continuous-variable quantum key distribution model. Each quantum forbidden-interval theorem gives a necessary and sufficient condition that determines whether stochastic resonance occurs in quantum communication of classical messages. The quantum theorems apply to any quantum noise source that has finite variance or that comes from the family of infinite-variance alpha-stable probability densities. Simulations show the predicted noise benefits for the basic quantum communication model and the continuous-variable quantum key distribution model.

PACS numbers: 03.67.−a, 03.67.Hk, 42.50.Dv, 05.45.Vx, 05.45.−a

(Some figures in this article are in colour only in the electronic version)

Stochastic resonance (SR) occurs in a nonlinear system when noise benefits the system [1–6]. SR can occur in both classical and quantum systems [4, 7] that use noise to help detect faint signals. The footprint of SR is a nonmonotonic curve that results when the system performance measure depends on the intensity of the noise source. Figure 1 shows such an SR surface for a quantum-optical communication system with both additive channel noise and squeezing noise. Mutual information measures the noise benefits of SR in bits [8–15].

The classical SR forbidden-interval theorems give necessary and sufficient conditions for an SR noise benefit when the system nonlinearity is a threshold [10, 11, 16] or is a soft threshold in a suitable stochastic differential equation [17]. The noise benefit turns on whether the noise mean or location a lies in an interval that depends on the threshold θ and the bipolar subthreshold signals A and $-A$: SR occurs if and only if $a \notin (\theta - A, \theta + A)$ where $-A < A < \theta$. This result holds for all finite-variance noise and all infinite-variance stable noise. But it guarantees only that some SR noise benefit occurs in the system for the given

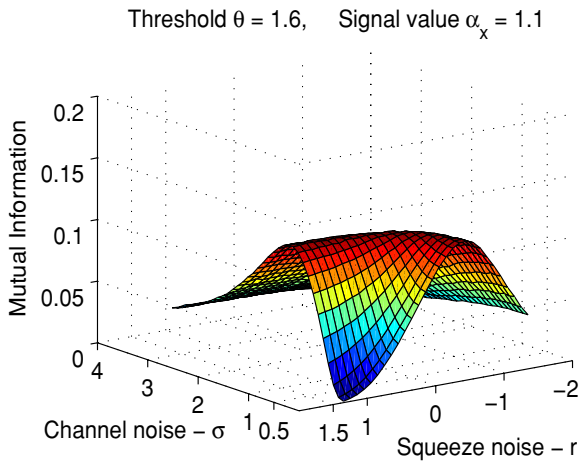

Figure 1. Stochastic resonance in quantum-optical communication with Gaussian noise. The sender Alice encodes coherent states with amplitude $A = 1.1$. The receiver Bob decodes with threshold $\theta = 1.6$. The graph shows the smoothed mutual information as a function of the standard deviation σ of the quantum Gaussian noise and the squeezing strength r for 100 simulation runs. Each run generated 10 000 input–output signal pairs to estimate the mutual information. The SR effect occurs because the channel noise mean $\mu = 0$ and lies outside the forbidden interval $(0.5, 2.7)$.

choice of parameters. SR stochastic learning algorithms [15, 16, 18, 19] can then search for the optimal noise level.

This paper generalizes the classical forbidden-interval theorems to quantum-optical communication with squeezed light [20, 21]. The quantum forbidden-interval theorems give necessary and sufficient conditions for a noise benefit and include the strength of light squeezing as a parameter. The quantum-optical system in figure 1 produces SR because the noise mean is zero and so does not lie in the system's forbidden interval $(0.5, 2.7)$. We also show that modified versions of the quantum forbidden-interval theorems hold in continuous-variable quantum key distribution with thresholding [22, 23]. These quantum SR systems still transmit classical binary information rather than quantum superposition or entanglement.

We structure this paper as follows. Section 1.1 presents the model of quantum communication with continuous variables. Section 1.2 briefly discusses how alpha-stable noise might occur in a quantum communication system. We prove two quantum forbidden-interval theorems in section 1.3 that apply to the model for quantum communication in section 1.1. The first theorem applies to the case of finite-variance noise and the second theorem applies to the case of infinite-variance alpha-stable noise. We introduce the model from [22, 23] for continuous-variable quantum key distribution (CVQKD) and include two strategies that an attacker may employ. We prove two quantum forbidden-interval theorems for the CVQKD model and conclude in section 3.

1. SR in continuous-variable quantum communication

1.1. Model for quantum-optical thresholding system

We first develop the basic quantum-optical communication protocol. We present the sender Alice's encoding operations, the effect of the noisy quantum channel on Alice's transmission, and the receiver Bob's detection scheme.

We describe our model in the Heisenberg picture. The protocol begins with Alice possessing a vacuum mode. Let $\hat{x}$ denote the position-quadrature operator of Alice's vacuum mode where $\hat{x} = (\hat{a}+\hat{a}^\dagger)/\sqrt{2}$ and $\hat{a}$ is the annihilation operator for her vacuum mode [21]. We consider only the position-quadrature operator's evolution. Her vacuum state collapses to a zero-mean $1/2$-variance Gaussian random variable X if she measures it with an ideal position-quadrature homodyne detector. Suppose that Alice does not measure it. Suppose instead that she sends her mode through a position-quadrature squeezer. Suppose further that she can control the strength of squeezing with a squeezing parameter r. The position-quadrature squeezer is the unitary operator $\hat{S}(r) \equiv \exp\{r(\hat{a}^2 - (\hat{a}^\dagger)^2)\}$ [21]. Her operator $\hat{x}$ evolves under the squeezer as $\hat{S}^\dagger(r)\hat{x}\hat{S}(r) = \hat{x}e^{-r}$. She encodes a message bit $S \in \{0, 1\}$ by displacing her state by $\alpha \in \mathbb{C}$ if $S = 1$ or by $-\alpha$ if $S = 0$. The displacement is the unitary operator $\hat{D}(\alpha) \equiv \exp\{\alpha\hat{a}^\dagger - \alpha^*\hat{a}\}$ [21]. Let α_S be the conditional displacement $\alpha_S = (-1)^{S+1}\alpha$. The Heisenberg-picture observable evolves under the displacement $\hat{D}(\alpha_S)$ as

$$\hat{D}^\dagger(\alpha_S)\hat{x}\hat{D}(\alpha_S) = \hat{x}e^{-r} + (-1)^{S+1}\alpha_x, \tag{1}$$

where $\alpha_x = \mathrm{Re}\{\alpha\}$ and the annihilation and creation operators in $\hat{D}(\alpha_S)$ equal respectively $\hat{a}\cosh r - \hat{a}^\dagger \sinh r$ and $\hat{a}^\dagger \cosh r - \hat{a}\sinh r$. The above equality gives the Heisenberg-picture observable that corresponds to Alice's mode before she sends it over the noisy channel. The message bit S appears as a displacement in (1).

Alice sends her mode to Bob over an additive noisy bosonic channel [24] that adds a random displacement $\nu \in \mathbb{C}$ to its input state. The channel randomly displaces any annihilation operator $\hat{a}$ as $\hat{D}^\dagger(\nu)\hat{a}\hat{D}(\nu) = \hat{a} + \nu$. This is the quantum-channel analog to a classical continuous additive noisy channel [25]. The term $\hat{x}e^{-r} + (-1)^{S+1}\alpha_x + \nu_x$ is the Heisenberg-picture position-quadrature observable that corresponds to the state that Bob receives after Alice sends her mode over the noisy channel. Random variable $\nu_x = \mathrm{Re}\{\nu\}$ and corresponds to the position-quadrature noise.

Bob detects the information that Alice encodes by performing position-quadrature homodyne detection with inefficient photodetectors. We model this non-ideal homodyne detection as lossy transmission through a material with linear absorption (a beamsplitter with transmittivity η) [26]. Then the Heisenberg-picture observable after the lossy beamsplitter is

$$\sqrt{\eta}((-1)^{S+1}\alpha_x + \hat{x}e^{-r} + \nu_x) + \sqrt{1-\eta}\hat{x}_H, \tag{2}$$

where $\hat{x}_H$ is the position quadrature operator of an input vacuum mode. Bob measures the position quadrature observable and the state collapses to the random variable

$$\sqrt{\eta}((-1)^{S+1}\alpha_x + Xe^{-r} + \nu_x) + \sqrt{1-\eta}X_H. \tag{3}$$

X_H is a zero-mean $1/2$-variance Gaussian random variable that corresponds to the vacuum observable $\hat{x}_H$. Random variables Xe^{-r}, ν_x, and X_H are independent because random variable Xe^{-r} comes from the vacuum fluctuations of Alice's original mode, because ν_x is Bob's (continuous) loss of knowledge due to the state's propagation through a noisy quantum channel, and because X_H comes from the vacuum contributions of non-ideal position-quadrature homodyne detection. Let random variable N sum all noise terms:

$$N \equiv \sqrt{\eta}(Xe^{-r} + \nu_x) + \sqrt{1-\eta}X_H. \tag{4}$$

The density $p_N(n)$ of random variable N is

$$p_N(n) = (p_{\sqrt{\eta}Xe^{-r}} * p_{\sqrt{\eta}\nu_x} * p_{\sqrt{1-\eta}X_H})(n), \tag{5}$$

where $p_{\sqrt{\eta}Xe^{-r}}(n)$ is the density of a zero-mean $\eta e^{-2r}/2$-variance Gaussian random variable, $p_{\sqrt{\eta}\nu_x}(n)$ is the density of $\sqrt{\eta}\nu_x$, $p_{\sqrt{1-\eta}X_H}(n)$ is the density of a zero-mean $(1-\eta)/2$-variance Gaussian random variable, and $*$ denotes convolution. The density $p_N(n)$ is a convolution

because random variables Xe^{-r}, ν_x and X_H are independent. So Bob's received signal using (3) and (4) is $\sqrt{\eta}(-1)^{S+1}\alpha_x + N$. Bob thresholds the result of the non-ideal homodyne detection with a threshold θ to retrieve a random bit Y where

$$Y \equiv u(\sqrt{\eta}(-1)^{S+1}\alpha_x + N - \theta) \tag{6}$$

and u is the step function defined as $u(x) = 1$ if $x \geqslant 0$ and $u(x) = 0$ if $x < 0$. Bob's detected bit Y should be the message bit S that Alice first sent.

We can also describe the above model in the Schrödinger picture. Alice sends either $\hat{D}(\alpha)\hat{S}(r)|0\rangle$ or $\hat{D}(-\alpha)\hat{S}(r)|0\rangle$. The noisy channel is the following completely positive trace-preserving map:

$$\rho \to \int p(\nu)\hat{D}(\nu)\rho\hat{D}^{\dagger}(\nu)\,\mathrm{d}\nu,$$

where $p(\nu)$ is the density of the noise. The positive measurement operators for ideal homodyne detection for Bob are as follows:

$$\Pi_{x<\theta} = \int_{x<\theta} |x\rangle\langle x|\,\mathrm{d}x,$$
$$\Pi_{x\geqslant\theta} = \int_{x\geqslant\theta} |x\rangle\langle x|\,\mathrm{d}x.$$

The results that one gets are the same as in the Heisenberg picture. But we use the Heisenberg picture because the analysis is more straightforward.

1.2. Quantum alpha-stable noise

The noise random variable ν_x need not have a finite second moment or finite higher-order moments. Some researchers argue that quantum-optical noise arises from a large number of independent random effects and thus that it is Gaussian because of the central limit theorem [27, 28]. But these random effects need not converge to a Gaussian random variable even though they converge to a random variable with a bell-curve density. The *generalized* central limit theorem states that all and only normalized stable random variables converge in distribution to a *stable* random variable [29]. So an impulsive quantum noise source may have a limiting alpha-stable density through aggregation or directly through transformation as when the Cauchy density arises from the tangent of uniform noise.

Alpha-stable noise models diverse physical phenomena such as impulsive interrupts in phone lines, underwater acoustics, low-frequency atmospheric signals, and gravitational fluctuations [30]. The parameter α (different from 'coherent state' α) lies in $(0, 2]$ and parametrizes the thickness of the curve's tails. The curve's tail thickness increases as α decreases: $\alpha = 1$ corresponds to the thick-tailed Cauchy random variable and $\alpha = 2$ corresponds to the familiar thin-tailed Gaussian random variable. The characteristic function $\varphi(\omega)$ of a general alpha-stable random variable is

$$\varphi(\omega) = \exp\{\mathrm{i}a\omega - \gamma|\omega|^{\alpha}(1 + \mathrm{i}\beta\,\mathrm{sign}(\omega)\tan(\alpha\pi/2))\},$$

for $\alpha \neq 1$ and

$$\varphi(\omega) = \exp\{\mathrm{i}a\omega - \gamma|\omega|(1 - 2\mathrm{i}\beta\,\mathrm{sign}(\omega)\ln(|\omega|)/\pi)\},$$

for $\alpha = 1$ where $\mathrm{sign}(\omega) = u(\omega) - u(-\omega)$, $\mathrm{i} = \sqrt{-1}$, $0 < \alpha \leqslant 2$, $-1 \leqslant \beta \leqslant 1$, and $\gamma > 0$. Parameter β is a skewness parameter such that $\beta = 0$ gives a symmetric density. Parameter γ controls the dispersion of the alpha-stable density around its location parameter a.

1.3. Quantum forbidden-interval theorems

Theorems 1 and 2 below show that any finite-variance quantum noise (not necessarily Gaussian) or any infinite-variance alpha-stable noise produces the SR effect. Theorem 1 states that the SR effect occurs for finite-variance noise if and only if the noise mean μ_{ν_x} falls outside the forbidden interval $(\theta - \alpha_x, \theta + \alpha_x)$. The noise location a replaces the noise mean in the forbidden-interval condition for infinite-variance noise in theorem 2. So adding noise in the form of squeezing noise, channel noise, and detector inefficiency noise can enhance performance. Figure 1 shows a simulation instance of the if-part of theorem 1.

The theorem states that the mutual information $I(S, Y)$ between sender and receiver tends to zero as all noise parameters decrease to zero. The mutual information $I(S, Y)$ is as follows [25]:

$$I(S, Y) \equiv \sum_{s,y} p_{S,Y}(s, y) \log \left(\frac{p_{S,Y}(s, y)}{p_S(s) p_Y(y)} \right).$$

The theorem assumes that the input and output signals are statistically dependent so that $I(S, Y) > 0$ [25]. So the SR effect occurs because the mutual information $I(S, Y)$ must increase away from zero as we add noise to the system: *what goes down must go up*.

Theorem 1. *Suppose the position quadrature ν_x of the noise has finite variance $\sigma^2_{\nu_x}$ and mean μ_{ν_x}. Suppose the input signal's position quadrature is subthreshold: $\alpha_x < \theta$. Suppose there is statistical dependence between input signal S and output signal Y so that the mutual information obeys $I(S, Y) > 0$. Then the quantum-optical system exhibits the nonmonotone SR effect if and only if the position quadrature of the noise mean does not lie in the forbidden interval: $\mu_{\nu_x} \notin (\theta - \alpha_x, \theta + \alpha_x)$. The nonmonotone SR effect is that $I(S, Y) \to 0$ as $\sigma^2_{\nu_x} \to 0$, as $r \to \infty$, and as $\eta \to 1$.*

Proof. The proof for sufficiency and necessity is similar to the respective proofs in [10, 11] if $p_N(n)$ is the noise density. Slight modifications of the proofs account for the homodyne efficiency η. See Appendix A.1. □

Theorem 2. *Suppose the position quadrature ν_x of the noise has dispersion γ and location a. Suppose the input signal's position quadrature is subthreshold: $\alpha_x < \theta$. Suppose there is statistical dependence between input signal S and output signal Y so that the mutual information obeys $I(S, Y) > 0$. Then the quantum-optical system exhibits the nonmonotone SR effect if and only if the position quadrature of the noise location does not lie in the forbidden interval: $a \notin (\theta - \alpha_x, \theta + \alpha_x)$. The nonmonotone SR effect is that $I(S, Y) \to 0$ as $\gamma \to 0$, as $r \to \infty$, and as $\eta \to 1$.*

Proof. The infinite-variance proof is similar to the respective α-stable proofs in [10, 11] if we use $p_N(n)$ as the noise density and if ν_x is an alpha-stable random variable. Slight modifications of the proofs again account for the homodyne efficiency η. See Appendix A.2. □

2. SR in continuous-variable quantum key distribution

Bennett and Brassard developed quantum key distribution as a way for two parties to establish a secret key [31]. Quantum key distribution has been the focus of much effort in quantum information processing for over 20 years. The recent review article by Scarani *et al* gives a broad overview of the current status of the field [32].

The original Bennett–Brassard proposal encoded information into discrete quantum variables. The authors have since extended this proposal to continuous quantum variables [32]. In particular, some authors have also shown that it is possible to create a 'mixed-signal' quantum key distribution protocol by thresholding a continuous quantum variable with a homodyne measurement to give a discrete-variable secret key [22, 23].

We show in this section that the SR effect occurs in the continuous-variable quantum key distribution (CVQKD) scenario from [22, 23]. We modify the form of the above forbidden-interval theorem to include the subtleties of the CVQKD model.

2.1. Model for CVQKD

We first present the model for CVQKD from [22, 23] without including the attacker Eve. Alice wants to send a secret bit S to Bob. Alice randomly sends one of four coherent states to Bob: $\{|\alpha\rangle, |\mathrm{i}\alpha\rangle, |-\alpha\rangle, |-\mathrm{i}\alpha\rangle\}$ where $\alpha \in \mathbb{R}^+$. Random bit $S = 0$ if she sends $|-\alpha\rangle$ or $|-\mathrm{i}\alpha\rangle$ and $S = 1$ if she sends $|\alpha\rangle$ or $|\mathrm{i}\alpha\rangle$. Bob randomly measures the state's position quadrature or momentum quadrature. Alice and Bob communicate classically after quantum communication ends. They divide the measurement results into 'correct-basis' and 'incorrect-basis'. The data are correct-basis if Bob measures the position quadrature when Alice sends $\{|\alpha\rangle, |-\alpha\rangle\}$ or if Bob measures the momentum quadrature when Alice sends $\{|\mathrm{i}\alpha\rangle, |-\mathrm{i}\alpha\rangle\}$. The data are incorrect-basis if it is not correct-basis. Alice and Bob keep only correct-basis data. Let $x \in \mathbb{R}$ be the result of Bob's measurement. Bob sets a threshold θ and assigns a bit value Y where $Y = 1$ if $x \geqslant \theta$, $Y = 0$ if $x \leqslant -\theta$, and $Y = \varepsilon$ otherwise. Symbol ε represents an inconclusive result.

Our analysis below corresponds only to correct-basis data because these data are crucial for determining the resulting performance of the protocol. We present the analysis only for the position-quadrature basis case. The same analysis holds for the momentum-quadrature case.

We now present a Heisenberg-picture analysis of the above model and include strategies that the attacker Eve can employ. The first few steps begin in the same way as the basic protocol above with Eve controlling the noisy channel. Then $\hat{x}e^{-r} + (-1)^{S+1}\alpha_x + \nu_x$ is the position-quadrature observable for the state that Eve possesses. She performs an amplifier-beamsplitter attack [33] by first passing the state through a phase-insensitive linear amplifier with gain $G \geqslant 1$ [34]. She then leaks a fraction $1 - \eta_E$ of the state through a beamsplitter so that Bob receives the fraction η_E. The Heisenberg-picture observable that corresponds to Bob's state is

$$\sqrt{\eta_E G}\hat{x}_s + \sqrt{\eta_E(G-1)}\hat{x}_{E_1} + \sqrt{1-\eta_E}\hat{x}_{E_2} \tag{7}$$

where $\hat{x}_s = \hat{x}e^{-r} + (-1)^{S+1}\alpha + \nu_x$. Modes $\hat{x}_{E_1}$ and $\hat{x}_{E_2}$ are vacuum modes resulting from the amplifier and beamsplitter and correspond to zero-mean $1/2$-variance Gaussian random variables upon measurement. Bob then measures the above operator by non-ideal position-quadrature homodyne detection. It collapses to the random variable $N + \sqrt{\eta_E\eta_B G}(-1)^{S+1}\alpha$ where N sums all noise terms,

$$N \equiv \sqrt{\eta_E\eta_B G}(Xe^{-r} + \nu_x) + \sqrt{\eta_E\eta_B(G-1)}X_{E_1} + \sqrt{\eta_B(1-\eta_E)}X_{E_2} + \sqrt{1-\eta_B}X_H,$$

η_B is the efficiency of Bob's homodyne detection, and X_H is a zero-mean $1/2$-variance Gaussian random variable that arises from homodyne detection noise. The density $p_N(n)$ of random variable N is

$$p_N(n) = (p_{\mathcal{N}(0,\sigma^2)} * p_{\sqrt{\eta_E\eta_B G}\nu_x})(n), \tag{8}$$

where $p_{\mathcal{N}(0,\sigma^2)}$ is the density of a zero-mean Gaussian random variable with variance

$$(\eta_B(\eta_E G e^{-2r} + \eta_E(G-1) + (1-\eta_E)) + 1 - \eta_B)/2$$

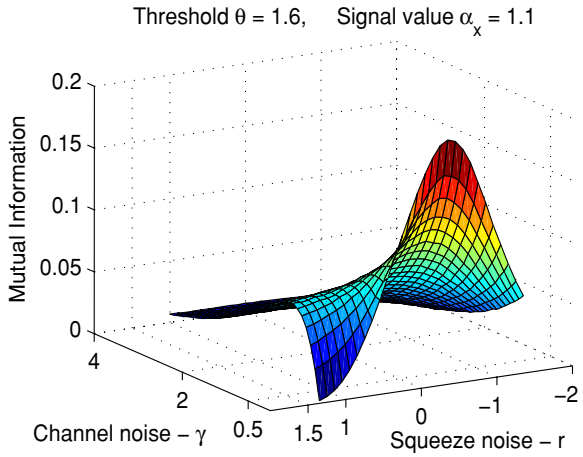

Figure 2. SR in continuous-variable quantum key distribution. Alice encodes coherent states with amplitude $A = 1.1$ and Bob decodes with threshold $\theta = 1.6$. The graph shows the smoothed mutual information as a function of the dispersion γ of infinite-variance quantum Cauchy noise and squeezing strength r for 100 simulation runs. We do not include amplifier, beamsplitter, or photodetector inefficiency noise. Each run generated 10 000 input–output signal pairs to estimate the mutual information. The SR effect occurs because the channel noise location $a = 0$ and so a lies outside the forbidden interval $(-2.7, -0.5) \cup (0.5, 2.7)$.

and $p_{\sqrt{\eta_E \eta_B G} v_x}$ is the density of $\sqrt{\eta_E \eta_B G} v_x$. Bob decodes with a threshold θ and gets a random bit Y where

$$Y = \begin{cases} 1 & : \quad N + \sqrt{\eta_E \eta_B G}(-1)^{S+1}\alpha \geqslant \theta \\ 0 & : \quad N + \sqrt{\eta_E \eta_B G}(-1)^{S+1}\alpha \leqslant -\theta \\ \varepsilon & : \quad \text{else} \end{cases} . \tag{9}$$

2.2. *Quantum forbidden-interval theorems for SR in CVQKD*

Protagonists Alice and Bob and antagonist Eve all play a role in the SR effect in CVQKD with thresholding. Alice adds Heisenberg noise in the form of squeezing. Eve adds channel, amplifier, and leakage noise in her attack. Bob adds photodetector inefficiency noise. The modified quantum forbidden-interval theorems characterize this interplay and give a necessary and sufficient condition for the SR effect for both finite-variance noise and infinite-variance alpha-stable noise. Figure 2 shows a simulation instance of the if-part of theorem 4.

Theorem 3. *Suppose the channel noise position quadrature has finite variance $\sigma^2_{v_x}$ and mean μ_{v_x}. Suppose the input signal's amplitude α is subthreshold: $\alpha < \theta$ and $-\alpha > -\theta$. Suppose there is some statistical dependence between input signal S and output signal Y so that the mutual information obeys $I(S, Y) > 0$. Then the quantum key distribution system exhibits the nonmonotone SR effect if and only if the position quadrature of the noise mean does not lie in the forbidden interval: $\mu_{v_x} \notin (-\theta - \alpha, -\theta + \alpha) \cup (\theta - \alpha, \theta + \alpha)$. The nonmonotone SR effect is that $I(S, Y) \to 0$ as $\sigma^2_{v_x} \to 0$, as $r \to \infty$, as $G \to 1$, as $\eta_E \to 1$, and as $\eta_B \to 1$.*

Proof. The proof method follows the proof of theorem 1 using $p_N(n)$ in (8). The proof requires three cases rather than two because the CVQKD model differs from the basic model. See Appendix B.1. □

Theorem 4. *Suppose the channel noise position quadrature has finite variance dispersion γ and location a. Suppose the input signal's amplitude α is subthreshold: $\alpha < \theta$ and $-\alpha > -\theta$. Suppose there is some statistical dependence between input signal S and output signal Y so that the mutual information obeys $I(S, Y) > 0$. Then the quantum key distribution system exhibits the nonmonotone SR effect if and only if the position quadrature of the noise location does not lie in the forbidden interval: $a \notin (-\theta - \alpha, -\theta + \alpha) \cup (\theta - \alpha, \theta + \alpha)$. The nonmonotone SR effect is that $I(S, Y) \to 0$ as $\gamma \to 0$, as $r \to \infty$, as $G \to 1$, as $\eta_E \to 1$, and as $\eta_B \to 1$.*

Proof. The proof method follows the proof of theorem 1 using $p_N(n)$ in (8). The proof requires three cases rather than two because the CVQKD model differs from the basic model. See Appendix B.2. □

3. Conclusion

Our quantum forbidden-interval theorems guarantee only that the nonmonotone SR effect occurs. They do not give the optimal combination of channel noise, squeezing, and photodetector noise. Nor do they guarantee a large increase in mutual information. The theorems also may not appear realistic because their proof requires infinite squeezing in the limit. But the theorems guarantee that the SR effect occurs for some finite squeezing. The simulations in both figures display the full nonmonotone SR signature for plausible squeezing values and for realistic channel noise levels.

The theorems may not appear 'quantum' because their proofs resemble those of the classical theorems. But they are 'quantum' because they use the non-classical effect of quantum squeezing and noise from a quantum source. The HSW coding theorem [35] likewise does not lose its 'quantum' status because its proof uses Shannon-theoretic techniques.

The SR result for CVQKD may also not appear practical. But what appears impractical today may be practical in the future when technology can better approximate the conditions of the theorem. The result shows that the CVQKD enjoys the SR effect because its nonlinear threshold structure resembles that of the model in theorem 1.

One may think that Alice and Bob should operate their CVQKD system with parameters that maximize their mutual information even for an optimal attack of the eavesdropper. But that may not be the best way for Alice and Bob to maximize their mutual information when the quantum channel is noisy because then noise can increase the QKD security [36].

Forbidden interval theorems may hold for more complex quantum systems. The quantum systems in this paper use noisy quantum processing to produce a mutual-information benefit between two classical variables. Other systems might use noise to enhance the coherence of a quantum state. The performance measure would be the coherent information [35]. The coherent information also relates to the capacity for sending private classical information [37]. This suggests further connections between SR and QKD and the potential for new learning algorithms that can locate noise optima.

Acknowledgments

The authors would like to thank Todd A Brun, Igor Devetak, Jonathan P Dowling and Austin Lund for helpful discussions. MMW acknowledges support from NSF grant CCF-0545845, the Army Research Office, and Disruptive Technologies Office.

Appendix A

Appendix A.1. Proof of theorem 1 (finite variance)

The proofs for sufficiency and necessity follow the respective proof methods in [10, 11] if we use (5) as the noise density.

Calculate first the four conditional probabilities $p_{Y|S}(0|0)$, $p_{Y|S}(0|1)$, $p_{Y|S}(1|0)$, $p_{Y|S}(1|1)$

$$\begin{aligned} p_{Y|S}(0|0) &= \Pr\{u(\sqrt{\eta}(-1)^{S+1}\alpha_x + N - \theta) = 0 \mid S = 0\} \\ &= \Pr\{\sqrt{\eta}(-1)^{S+1}\alpha_x + N - \theta < 0 \mid S = 0\} \\ &= \Pr\{-\sqrt{\eta}\alpha_x + N < \theta\} = \Pr\{N < \theta + \sqrt{\eta}\alpha_x\} \\ &= \int_{-\infty}^{\theta+\sqrt{\eta}\alpha_x} p_N(n)\, \mathrm{d}n. \end{aligned} \tag{A.1}$$

The other conditional probabilities follow from similar calculations:

$$p_{Y|S}(0|1) = \int_{-\infty}^{\theta-\sqrt{\eta}\alpha_x} p_N(n)\, \mathrm{d}n, \tag{A.2}$$

$$p_{Y|S}(1|0) = \int_{\theta+\sqrt{\eta}\alpha_x}^{\infty} p_N(n)\, \mathrm{d}n, \tag{A.3}$$

$$p_{Y|S}(1|1) = \int_{\theta-\sqrt{\eta}\alpha_x}^{\infty} p_N(n)\, \mathrm{d}n. \tag{A.4}$$

Proof (Sufficiency). Assume that $0 < p_S(s) < 1$ to avoid triviality when $p_S(s) = 0$ or 1. $I(S, Y) = 0$ if and only if S and Y are statistically independent [25]. We show that S and Y are asymptotically independent: $I(S, Y) \to 0$ as $\sigma^2_{\nu_x} \to 0$, as $r \to \infty$, and as $\eta \to 1$. The following definition holds for the proofs that follows:

$$\sigma^2 \equiv \eta(e^{-2r}/2 + \sigma^2_{\nu_x}) + (1 - \eta)/2 \tag{A.5}$$

We need to show that $p_{Y|S}(y|s) = p_Y(y)$ as $\sigma^2_{\nu_x} \to 0$, as $r \to \infty$, and as $\eta \to 1$ for $s, y \in \{0, 1\}$. Consider an algebraic manipulation using the law of total probability:

$$\begin{aligned} p_Y(y) &= \sum_s p_{Y|S}(y|s)\ p_S(s) \\ &= p_{Y|S}(y|0)\ p_S(0) + p_{Y|S}(y|1)\ p_S(1) \\ &= p_{Y|S}(y|0)\ p_S(0) + p_{Y|S}(y|1)\ (1 - p_S(0)) \\ &= (p_{Y|S}(y|0) - p_{Y|S}(y|1))p_S(0) + p_{Y|S}(y|1). \end{aligned} \tag{A.6}$$

We can show by a similar method that

$$p_Y(y) = (p_{Y|S}(y|1) - p_{Y|S}(y|0))p_S(1) + p_{Y|S}(y|0).$$

So $p_Y(y) \to p_{Y|S}(y|1)$ and $p_Y(y) \to p_{Y|S}(y|0)$ as $p_{Y|S}(y|1) - p_{Y|S}(y|0) \to 0$. Consider the case where $y = 0$

$$p_{Y|S}(0|0) - p_{Y|S}(0|1) = \int_{\theta-\sqrt{\eta}\alpha_x}^{\theta+\sqrt{\eta}\alpha_x} p_N(n)\, \mathrm{d}n.$$

Consider the case where $y = 1$:

$$p_{Y|S}(1|0) - p_{Y|S}(1|1) = -\int_{\theta-\sqrt{\eta}\alpha_x}^{\theta+\sqrt{\eta}\alpha_x} p_N(n)\, \mathrm{d}n.$$

So the result follows if

$$\int_{\theta-\sqrt{\eta}\alpha_x}^{\theta+\sqrt{\eta}\alpha_x} p_N(n)\,\mathrm{d}n \to 0 \tag{A.7}$$

as $\sigma_{v_x}^2 \to 0$, as $r \to \infty$, and as $\eta \to 1$. Now

$$\mu_{v_x} \notin (\theta - \alpha_x, \theta + \alpha_x)$$

by hypothesis. We ignore the zero-measure cases where $\mu_{v_x} = \theta - \alpha_x$ or $\mu_{v_x} = \theta + \alpha_x$.

Case 1. Suppose first that $\mu_{v_x} < \theta - \alpha_x$. So $\mu_{v_x} + \alpha_x < \theta$ and thus

$$\sqrt{\eta}(\mu_{v_x} + \alpha_x) \leqslant \mu_{v_x} + \alpha_x < \theta$$

for any $\eta \in (0, 1]$. Pick

$$\epsilon = \frac{1}{2}(\theta - \sqrt{\eta}\alpha_x - \sqrt{\eta}\mu_{v_x}) > 0.$$

So $\theta - \sqrt{\eta}\alpha_x - \epsilon = \sqrt{\eta}\mu_x + \epsilon$. Then

$$\begin{aligned}
\int_{\theta-\sqrt{\eta}\alpha_x}^{\theta+\sqrt{\eta}\alpha_x} p_N(n)\,\mathrm{d}n &\leqslant \int_{\theta-\sqrt{\eta}\alpha_x}^{\infty} p_N(n)\,\mathrm{d}n \\
&\leqslant \int_{\theta-\sqrt{\eta}\alpha_x-\epsilon}^{\infty} p_N(n)\,\mathrm{d}n \\
&\leqslant \int_{\sqrt{\eta}\mu_{v_x}+\epsilon}^{\infty} p_N(n)\,\mathrm{d}n \\
&= \Pr\{N \geqslant \sqrt{\eta}\mu_{v_x} + \epsilon\} \\
&= \Pr\{N \geqslant \mu + \epsilon\} \\
&= \Pr\{N - \mu \geqslant \epsilon\} \\
&\leqslant \Pr\{|N - \mu| \geqslant \epsilon\} \\
&\leqslant \frac{\sigma^2}{\epsilon^2}
\end{aligned}$$

by the Chebyshev inequality.

So the result follows when $\mu_{v_x} < \theta - \alpha_x$ because $p_{Y|S}(0|0) - p_{Y|S}(0|1) \to 0$ as $\sigma_{v_x}^2 \to 0$, as $r \to \infty$, and as $\eta \to 1$.

Case 2. Suppose next that $\mu_{v_x} > \theta + \alpha_x$ so that $\mu_{v_x} - \alpha_x > \theta > 0$. Choose $\sqrt{\eta}$ large enough so that

$$\sqrt{\eta} > \theta/(\mu_{v_x} - \alpha_x).$$

So $\sqrt{\eta}(\mu_{v_x} - \alpha_x) > \theta$. Pick

$$\epsilon = \frac{1}{2}(\sqrt{\eta}\mu_{v_x} - \theta - \sqrt{\eta}\alpha_x) > 0.$$

So $\theta + \sqrt{\eta}\alpha_x + \epsilon = \sqrt{\eta}\mu_{v_x} - \epsilon$. Then

$$\begin{aligned}
\int_{\theta-\sqrt{\eta}\alpha_x}^{\theta+\sqrt{\eta}\alpha_x} p_N(n)\,\mathrm{d}n &\leqslant \int_{-\infty}^{\theta+\sqrt{\eta}\alpha_x} p_N(n)\,\mathrm{d}n \\
&\leqslant \int_{-\infty}^{\theta+\sqrt{\eta}\alpha_x+\epsilon} p_N(n)\,\mathrm{d}n \\
&\leqslant \int_{-\infty}^{\sqrt{\eta}\mu_{v_x}-\epsilon} p_N(n)\,\mathrm{d}n
\end{aligned}$$

$$
\begin{aligned}
&= \Pr\{N \leqslant \sqrt{\eta}\mu_{v_x} - \epsilon\} \\
&= \Pr\{N \leqslant \mu - \epsilon\} \\
&= \Pr\{N - \mu \leqslant -\epsilon\} \\
&\leqslant \Pr\{|N - \mu| \geqslant \epsilon\} \\
&\leqslant \frac{\sigma^2}{\epsilon^2}.
\end{aligned}
$$

So $p_{Y|S}(0|0) - p_{Y|S}(0|1) \to 0$ as $\sigma^2_{v_x} \to 0$, as $r \to \infty$, and as $\eta \to 1$ when $\mu_{v_x} > \theta + \alpha_x$. Thus

$$\mu_{v_x} \notin (\theta - \alpha_x, \theta + \alpha_x)$$

is a sufficient condition for the nonmonotone SR effect to occur. □

Proof (Necessity). The system does not exhibit the nonmonotone SR effect if $\mu_{v_x} \in (\theta - \alpha_x, \theta + \alpha_x)$ in the sense that $I(S,Y)$ is maximum as $\sigma^2_{v_x} \to 0$, as $r \to \infty$, and as $\eta \to 1$. $I(S, Y) \to H(Y) = H(S)$ as $\sigma^2_{v_x} \to 0$, as $r \to \infty$, and as $\eta \to 1$. Assume that $0 < p_S(s) < 1$ to avoid triviality when $p_S(s) = 0$ or 1. We show that $H(Y) \to H(S)$ and $H(Y|S) \to 0$ as $\sigma^2_{v_x} \to 0$, as $r \to \infty$, and as $\eta \to 1$. It is maximum in this limit because $I(S, Y) = H(Y) - H(Y|S)$ and $I(S, Y) \leqslant H(S)$ by the data processing inequality for a Markov chain [25]. Consider the conditional entropy $H(Y|S)$:

$$
\begin{aligned}
H(Y|S) &= -\sum_{s,y} p_{Y,S}(y, s) \log_2 p_{Y|S}(y|s) \\
&= -\sum_s p_S(s) \sum_y p_{Y|S}(y|s) \log_2 p_{Y|S}(y|s). \qquad \text{(A.8)}
\end{aligned}
$$

Suppose for now that $p_{Y|S}(y|s) \to 1$ or 0 for all $s, y \in \{0, 1\}$ as $\sigma^2_{v_x} \to 0$, as $r \to \infty$, and as $\eta \to 1$. Then $H(Y|S) \to 0$ by inspecting (A.8) and applying $1 \log_2 1 = 0$ and $0 \log_2 0 = 0$ by L'Hôspital's rule. So we will prove that each of the conditional probabilities vanishes or approaches 1 in the above limit if $\mu_{v_x} \in (\theta - \alpha_x, \theta + \alpha_x)$. Consider first $p_{Y|S}(0|0)$. Pick any $\mu_{v_x} \in (\theta - \alpha_x, \theta + \alpha_x)$. Then $\theta + \alpha_x - \mu_{v_x} > 0$ and $\theta > \mu_{v_x} - \alpha_x$. Then $\theta > \sqrt{\eta}(\mu_{v_x} - \alpha_x)$ for any $\eta \in (0, 1]$. Pick $\epsilon = \frac{1}{2}(\theta + \sqrt{\eta}\alpha_x - \sqrt{\eta}\mu_{v_x}) > 0$ so that $\theta + \sqrt{\eta}\alpha_x - \epsilon = \sqrt{\eta}\mu_{v_x} + \epsilon$:

$$
\begin{aligned}
p_{Y|S}(0|0) &= \int_{-\infty}^{\theta+\sqrt{\eta}\alpha_x} p_N(n)\, \mathrm{d}n \\
&\geqslant \int_{-\infty}^{\theta+\sqrt{\eta}\alpha_x-\epsilon} p_N(n)\, \mathrm{d}n \\
&= \int_{-\infty}^{\sqrt{\eta}\mu_{v_x}+\epsilon} p_N(n)\, \mathrm{d}n \\
&= 1 - \int_{\sqrt{\eta}\mu_{v_x}+\epsilon}^{\infty} p_N(n)\, \mathrm{d}n \\
&= 1 - \Pr\{N \geqslant \sqrt{\eta}\mu_{v_x} + \epsilon\} \\
&= 1 - \Pr\{N \geqslant \mu + \epsilon\} \\
&= 1 - \Pr\{N - \mu \geqslant \epsilon\} \\
&\geqslant 1 - \Pr\{|N - \mu| \geqslant \epsilon\} \\
&\geqslant 1 - \frac{\sigma^2}{\epsilon^2} \\
&\to 1
\end{aligned}
$$

as $\sigma_{v_x}^2 \to 0$, as $r \to \infty$, and as $\eta \to 1$. We prove the result similarly for $p_{Y|S}(1|1)$. Pick any $\mu_{v_x} \in (\theta - \alpha_x, \theta + \alpha_x)$. Then $\mu_{v_x} > \theta - \alpha_x$ and $\mu_{v_x} + \alpha_x > \theta > 0$. Suppose that η is large enough so that $\sqrt{\eta} > \theta/(\mu_{v_x} + \alpha_x)$. Then $\sqrt{\eta}(\mu_{v_x} + \alpha_x) > \theta$ and $\sqrt{\eta}\mu_{v_x} + \sqrt{\eta}\alpha_x - \theta > 0$. Pick $\epsilon = \frac{1}{2}(\sqrt{\eta}\mu_{v_x} + \sqrt{\eta}\alpha_x - \theta) > 0$ so that $\theta - \sqrt{\eta}\alpha_x + \epsilon = \sqrt{\eta}\mu_{v_x} - \epsilon$.

$$\begin{aligned}
p_{Y|S}(1|1) &= \int_{\theta - \sqrt{\eta}\alpha_x}^{\infty} p_N(n)\, \mathrm{d}n \\
&\geqslant \int_{\theta - \sqrt{\eta}\alpha_x + \epsilon}^{\infty} p_N(n)\, \mathrm{d}n \\
&= \int_{\sqrt{\eta}\mu_{v_x} - \epsilon}^{\infty} p_N(n)\, \mathrm{d}n \\
&= 1 - \int_{-\infty}^{\sqrt{\eta}\mu_{v_x} - \epsilon} p_N(n)\, \mathrm{d}n \\
&= 1 - \Pr\{N \leqslant \sqrt{\eta}\mu_{v_x} - \epsilon\} \\
&= 1 - \Pr\{N \leqslant \mu - \epsilon\} \\
&= 1 - \Pr\{N - \mu \leqslant -\epsilon\} \\
&\geqslant 1 - \Pr\{|N - \mu| \geqslant \epsilon\} \\
&\geqslant 1 - \frac{\sigma^2}{\epsilon^2} \\
&\to 1
\end{aligned}$$

as $\sigma_{v_x}^2 \to 0$, as $r \to \infty$, and as $\eta \to 1$. So $p_{Y|S}(0|0) \to 1$, $p_{Y|S}(1|1) \to 1$, $p_{Y|S}(1|0) \to 0$, and $p_{Y|S}(0|1) \to 0$ as $\sigma_{v_x}^2 \to 0$, as $r \to \infty$, and as $\eta \to 1$. The system does not display the nonmonotone SR effect. □

Appendix A.2. Proof of theorem 2 (infinite variance)

The proofs for sufficiency and necessity follow the respective stable proof methods in [10, 11] if we use (5) as the noise density and if v_x is an alpha-stable random variable.

The characteristic function $\varphi_{v_x}(\omega)$ of an alpha-stable noise source with density $p_{v_x}(n)$ is as follows:

$$\varphi_{v_x}(\omega) = \exp\left\{\mathrm{i}a\omega - \gamma|\omega|^{\alpha}\left(1 + \mathrm{i}\beta\,\mathrm{sign}(\omega)\tan\left(\frac{\alpha\pi}{2}\right)\right)\right\}, \tag{A.9}$$

where α is the characteristic exponent and β is a skewness parameter. So the characteristic function of $p_N(n)$ is as follows:

$$\begin{aligned}
\varphi_N(\omega) &= (\varphi_{\sqrt{\eta}Xe^{-r}} \cdot \varphi_{\sqrt{\eta}v_x} \cdot \varphi_{\sqrt{1-\eta}X_H})(\omega) \\
&= \exp\left\{-\frac{\eta e^{-2r}\omega^2}{4}\right\} \varphi_{v_x}(\sqrt{\eta}\omega) \exp\left\{-\frac{(1-\eta)\omega^2}{4}\right\} \\
&= \varphi_{v_x}(\sqrt{\eta}\omega) \exp\left\{-\frac{(\eta e^{-2r} + 1 - \eta)\omega^2}{4}\right\}
\end{aligned} \tag{A.10}$$

from (5) and the convolution theorem because the random variables are independent.

Proof (Sufficiency). Take the limit of the characteristic function $\varphi_N(\omega)$ as the dispersion $\gamma \to 0$, as squeezing parameter $r \to \infty$, and as homodyne efficiency $\eta \to 1$ to obtain the following characteristic function:

$$\lim_{r \to \infty, \gamma \to 0, \eta \to 1} \varphi_N(\omega) = \exp\{\mathrm{i}a\omega\}. \tag{A.11}$$

The probability density $p_N(n)$ then approaches a translated delta function

$$\lim_{r\to\infty,\gamma\to 0,\eta\to 1} p_N(n) = \delta(n-a). \tag{A.12}$$

The conditional probability difference obeys

$$p_{Y|S}(0|0) - p_{Y|S}(0|1) = \int_{\theta-\sqrt{\eta}\alpha_x}^{\theta+\sqrt{\eta}\alpha_x} p_N(n)\,\mathrm{d}n \tag{A.13}$$

$$\leqslant \int_{\theta-\alpha_x}^{\theta+\alpha_x} p_N(n)\,\mathrm{d}n. \tag{A.14}$$

Pick $a \notin (\theta-\alpha_x, \theta+\alpha_x)$. Consider the following limit:

$$\lim_{r\to\infty,\gamma\to 0,\eta\to 1} p_{Y|S}(0|0) - p_{Y|S}(0|1) \tag{A.15}$$

$$\leqslant \lim_{r\to\infty,\gamma\to 0,\eta\to 1} \int_{\theta-\alpha_x}^{\theta+\alpha_x} p_N(n)\,\mathrm{d}n \tag{A.16}$$

$$= \int_{\theta-\alpha_x}^{\theta+\alpha_x} \delta(n-a)\,\mathrm{d}n = 0 \tag{A.17}$$

because $a \notin (\theta-\alpha_x, \theta+\alpha_x)$. □

Proof (Necessity). Choose $a \in (\theta-\alpha_x, \theta+\alpha_x)$. Then

$$p_{Y|S}(0|0) = \int_{-\infty}^{\theta+\sqrt{\eta}\alpha_x} p_N(n)\,\mathrm{d}n \tag{A.18}$$

$$= \int_{-\infty}^{\theta} p_N(n+\sqrt{\eta}\alpha_x)\,\mathrm{d}n \tag{A.19}$$

$$\to \int_{-\infty}^{\theta} \delta(n-a+\alpha_x)\,\mathrm{d}n \tag{A.20}$$

$$= \int_{-\infty}^{\theta+\alpha_x} \delta(n-a)\,\mathrm{d}n = 1 \tag{A.21}$$

$$\text{as } \gamma\to 0, \text{ as } r\to\infty, \text{ and as } \eta\to 1 \tag{A.22}$$

$$p_{Y|S}(1|1) = \int_{\theta-\sqrt{\eta}\alpha_x}^{\infty} p_N(n)\,\mathrm{d}n \tag{A.23}$$

$$= \int_{\theta}^{\infty} p_N(n-\sqrt{\eta}\alpha_x)\,\mathrm{d}n \tag{A.24}$$

$$\to \int_{\theta}^{\infty} \delta(n-a_x-\alpha_x)\,\mathrm{d}n \tag{A.25}$$

$$= \int_{\theta-\alpha_x}^{\infty} \delta(n-a_x)\,\mathrm{d}n = 1 \tag{A.26}$$

$$\text{as } \gamma\to 0, \text{ as } r\to\infty, \text{ and as } \eta\to 1. \tag{A.27}$$

□

Appendix B

Appendix B.1. Proof of theorem 3 (finite variance)

Use the following shorthand for the proofs that follow:

$$\eta \equiv \eta_E \eta_B G.$$

The proofs use this shorthand when we take a limit in the parameters η_E, η_B and G. The mean μ and variance σ^2 of noise random variable N are $\mu = \sqrt{\eta}\mu_{v_x}$ and

$$\sigma^2 = \eta\sigma_{v_x}^2 + \left(\eta_B \left(\begin{array}{c} \eta_E G e^{-2r} + \eta_E(G-1) \\ +(1-\eta_E) \end{array} \right) + 1 - \eta_B\right) \Big/ 2. \tag{B.1}$$

We compute the six conditional probabilities: $p_{Y|S}(0|0)$, $p_{Y|S}(0|1)$, $p_{Y|S}(1|0)$, $p_{Y|S}(1|1)$, $p_{Y|S}(\varepsilon|0)$, and $p_{Y|S}(\varepsilon|1)$

$$\begin{aligned} p_{Y|S}(0|0) &= \Pr\{N + \sqrt{\eta}(-1)^{S+1}\alpha \leqslant -\theta \mid S = 0\} \\ &= \Pr\{-\sqrt{\eta}\alpha + N \leqslant -\theta\} \\ &= \Pr\{N < -\theta + \sqrt{\eta}\alpha\} \\ &= \int_{-\infty}^{-\theta+\sqrt{\eta}\alpha} p_N(n)\, \mathrm{d}n. \end{aligned} \tag{B.2}$$

The other conditional probabilities follow from similar reasoning:

$$p_{Y|S}(0|1) = \int_{-\infty}^{-\theta-\sqrt{\eta}\alpha} p_N(n)\, \mathrm{d}n, \tag{B.3}$$

$$p_{Y|S}(1|0) = \int_{\theta+\sqrt{\eta}\alpha}^{\infty} p_N(n)\, \mathrm{d}n, \tag{B.4}$$

$$p_{Y|S}(1|1) = \int_{\theta-\sqrt{\eta}\alpha}^{\infty} p_N(n)\, \mathrm{d}n, \tag{B.5}$$

$$\begin{aligned} p_{Y|S}(\varepsilon|0) &= 1 - p_{Y|S}(0|0) - p_{Y|S}(1|0) \\ &= \int_{-\theta+\sqrt{\eta}\alpha}^{\theta+\sqrt{\eta}\alpha} p_N(n)\, \mathrm{d}n, \end{aligned} \tag{B.6}$$

$$\begin{aligned} p_{Y|S}(\varepsilon|1) &= 1 - p_{Y|S}(0|1) - p_{Y|S}(1|1) \\ &= \int_{-\theta-\sqrt{\eta}\alpha}^{\theta-\sqrt{\eta}\alpha} p_N(n)\, \mathrm{d}n. \end{aligned} \tag{B.7}$$

Proof (Sufficiency). We follow the proof method of theorem 1 with some modifications. Note that the conditions $\eta_E, \eta_B \leqslant 1$ and $G \geqslant 1$ constrain how we take both limits to one. This constrains the values that the root of their product $\sqrt{\eta}$ may take for any given value of the noise mean μ_{v_x}. Assume these constraints when considering the limit in the proofs that follow.

Assume that $0 < p_S(s) < 1$ to avoid triviality when $p_S(s) = 0$ or 1. $I(S, Y) = 0$ if and only if S and Y are statistically independent [25]. We show that S and Y are asymptotically independent: $I(S, Y) \to 0$ as $\sigma_{v_x}^2 \to 0$, as $r \to \infty$, as $\eta \to 1$, and as $G \to 1$. We need to show that $p_{Y|S}(y|s) \to p_Y(y)$ as $\sigma_{v_x}^2 \to 0$, as $r \to \infty$, as $\eta \to 1$, and as $G \to 1$ for $s, y \in \{0, 1\}$. We do not consider $p_{Y|S}(y|\varepsilon)$ because the probability $p_S(\varepsilon)$ is zero and so the probability

$p_Y(\varepsilon)$ is also zero. Consider the expansion in (A.6) using the law of total probability. The expansion is the same even when including symbol ε because ε has zero probability: $p_S(\varepsilon) = 0$. So $p_Y(y) \to p_{Y|S}(y|1)$ and $p_Y(y) \to p_{Y|S}(y|0)$ as $p_{Y|S}(0|0) - p_{Y|S}(0|1) \to 0$ and $p_{Y|S}(1|1) - p_{Y|S}(1|0) \to 0$. Consider the case where $y = 0$:

$$p_{Y|S}(0|0) - p_{Y|S}(0|1) = \int_{-\theta-\sqrt{\eta}\alpha}^{-\theta+\sqrt{\eta}\alpha} p_N(n)\, \mathrm{d}n. \tag{B.8}$$

Consider the case where $y = 1$:

$$p_{Y|S}(1|1) - p_{Y|S}(1|0) = \int_{\theta-\sqrt{\eta}\alpha}^{\theta+\sqrt{\eta}\alpha} p_N(n)\, \mathrm{d}n. \tag{B.9}$$

So the result follows if both of the above conditional probability differences vanish as $\sigma_{v_x}^2 \to 0$, as $r \to \infty$, as $\eta_E, \eta_B \to 1$, and as $G \to 1$. Suppose the mean $\mu_{v_x} \notin (-\theta - \alpha, -\theta + \alpha) \cup (\theta - \alpha, \theta + \alpha)$ by hypothesis. We ignore the zero-measure cases where $\mu_{v_x} = \theta - \alpha$, $\mu_{v_x} = \theta + \alpha$, $\mu_{v_x} = -\theta + \alpha$, or $\mu_{v_x} = -\theta - \alpha$.

Case 1. Suppose first that $\mu_{v_x} < -\theta - \alpha$. So $\mu_{v_x} + \alpha < -\theta$ and thus $\sqrt{\eta}(\mu_{v_x} + \alpha) \leqslant \mu_{v_x} + \alpha < -\theta$ whenever $\sqrt{\eta} > -\theta/(\mu_{v_x} + \alpha) = \theta/|\mu_{v_x} + \alpha|$. Pick $\epsilon = \frac{1}{2}(-\theta - \sqrt{\eta}\alpha - \sqrt{\eta}\mu_{v_x}) > 0$. So $-\theta - \sqrt{\eta}\alpha - \epsilon = \sqrt{\eta}\mu_{v_x} + \epsilon$. Then

$$\begin{aligned}
\int_{-\theta-\sqrt{\eta}\alpha}^{-\theta+\sqrt{\eta}\alpha} p_N(n)\, \mathrm{d}n &\leqslant \int_{-\theta-\sqrt{\eta}\alpha}^{\infty} p_N(n)\, \mathrm{d}n \\
&\leqslant \int_{-\theta-\sqrt{\eta}\alpha-\epsilon}^{\infty} p_N(n)\, \mathrm{d}n \\
&\leqslant \int_{\sqrt{\eta}\mu_{v_x}+\epsilon}^{\infty} p_N(n)\, \mathrm{d}n \\
&= \Pr\{N \geqslant \sqrt{\eta}\mu_{v_x} + \epsilon\} \\
&= \Pr\{N \geqslant \mu + \epsilon\} \\
&= \Pr\{N - \mu \geqslant \epsilon\} \\
&\leqslant \Pr\{|N - \mu| \geqslant \epsilon\} \\
&\leqslant \frac{\sigma^2}{\epsilon^2}.
\end{aligned}$$

So the conditional probability difference in (B.8) vanishes as $\sigma_{v_x}^2 \to 0$, as $r \to \infty$, as $\eta_E, \eta_B \to 1$, and as $G \to 1$ when $\mu_{v_x} < -\theta - \alpha$. We now prove that the conditional probability difference in (B.9) vanishes when $\mu_{v_x} < -\theta - \alpha$. It follows that $\mu_{v_x} < \theta - \alpha$ if $\mu_{v_x} < -\theta - \alpha$. So $\mu_{v_x} + \alpha < \theta$ and thus $\sqrt{\eta}(\mu_{v_x} + \alpha) \leqslant \mu_{v_x} + \alpha < \theta$ for any $\sqrt{\eta} \geqslant 0$ because $\mu_{v_x} + \alpha < 0$. Pick $\epsilon = \frac{1}{2}(\theta - \sqrt{\eta}\alpha - \sqrt{\eta}\mu_{v_x}) > 0$. So $\theta - \sqrt{\eta}\alpha - \epsilon = \sqrt{\eta}\mu_{v_x} + \epsilon$. Then

$$\begin{aligned}
\int_{\theta-\sqrt{\eta}\alpha}^{\theta+\sqrt{\eta}\alpha} p_N(n)\, \mathrm{d}n &\leqslant \int_{\theta-\sqrt{\eta}\alpha}^{\infty} p_N(n)\, \mathrm{d}n \\
&\leqslant \int_{\theta-\sqrt{\eta}\alpha-\epsilon}^{\infty} p_N(n)\, \mathrm{d}n \\
&\leqslant \int_{\sqrt{\eta}\mu_{v_x}+\epsilon}^{\infty} p_N(n)\, \mathrm{d}n \\
&= \Pr\{N \geqslant \sqrt{\eta}\mu_{v_x} + \epsilon\} \\
&= \Pr\{N \geqslant \mu + \epsilon\}
\end{aligned}$$

$$\begin{aligned}
&= \Pr\{N - \mu \geqslant \epsilon\} \\
&\leqslant \Pr\{|N - \mu| \geqslant \epsilon\} \\
&\leqslant \frac{\sigma^2}{\epsilon^2}.
\end{aligned}$$

So the conditional probability difference in (B.9) vanishes as $\sigma_{\nu_x}^2 \to 0$, as $r \to \infty$, as $\eta_E, \eta_B \to 1$, and as $G \to 1$ when $\mu_{\nu_x} < -\theta - \alpha$ and with constraint $\sqrt{\eta} > \theta/|\mu_{\nu_x} + \alpha|$.

Case 2. Suppose next that $-\theta+\alpha < \mu_{\nu_x} < \theta-\alpha$. We first prove that the conditional probability difference in (B.8) vanishes as $\sigma_{\nu_x}^2 \to 0$, as $r \to \infty$, as $\eta_E, \eta_B \to 1$, and as $G \to 1$. So $\mu_{\nu_x} - \alpha > -\theta$ if $-\theta + \alpha < \mu_{\nu_x} < \theta - \alpha$. Thus $\sqrt{\eta}(\mu_{\nu_x} - \alpha) \geqslant \mu_{\nu_x} - \alpha > -\theta$ whenever $\sqrt{\eta} < \theta/|\mu_{\nu_x} - \alpha|$. Pick $\epsilon = \frac{1}{2}(\theta - \sqrt{\eta}\alpha + \sqrt{\eta}\mu_{\nu_x}) > 0$. So $-\theta + \sqrt{\eta}\alpha + \epsilon = \sqrt{\eta}\mu_{\nu_x} - \epsilon$. Then

$$\begin{aligned}
\int_{-\theta-\sqrt{\eta}\alpha}^{-\theta+\sqrt{\eta}\alpha} p_N(n)\, \mathrm{d}n &\leqslant \int_{-\infty}^{-\theta+\sqrt{\eta}\alpha} p_N(n)\, \mathrm{d}n \\
&\leqslant \int_{-\infty}^{-\theta+\sqrt{\eta}\alpha+\epsilon} p_N(n)\, \mathrm{d}n \\
&\leqslant \int_{-\infty}^{\sqrt{\eta}\mu_{\nu_x}-\epsilon} p_N(n)\, \mathrm{d}n \\
&= \Pr\{N \leqslant \sqrt{\eta}\mu_{\nu_x} - \epsilon\} \\
&= \Pr\{N \leqslant \mu - \epsilon\} \\
&= \Pr\{N - \mu \leqslant -\epsilon\} \\
&\leqslant \Pr\{|N - \mu| \geqslant \epsilon\} \\
&\leqslant \frac{\sigma^2}{\epsilon^2}.
\end{aligned}$$

So the conditional probability difference in (B.8) vanishes as $\sigma_{\nu_x}^2 \to 0$, as $r \to \infty$, as $\eta_E, \eta_B \to 1$, and as $G \to 1$ when $-\theta + \alpha < \mu_{\nu_x} < \theta - \alpha$. We now prove that the conditional probability difference in (B.9) vanishes as $\sigma_{\nu_x}^2 \to 0$, as $r \to \infty$, as $\eta_E, \eta_B \to 1$, and as $G \to 1$. So $\mu_{\nu_x} + \alpha < \theta$ if $-\theta + \alpha < \mu_{\nu_x} < \theta - \alpha$. Thus $\sqrt{\eta}(\mu_{\nu_x} + \alpha) \leqslant \mu_{\nu_x} + \alpha < \theta$ whenever $\sqrt{\eta} < \theta/|\mu_{\nu_x} + \alpha|$. Pick $\epsilon = \frac{1}{2}(\theta - \sqrt{\eta}\alpha - \sqrt{\eta}\mu_{\nu_x}) > 0$. So $\theta - \sqrt{\eta}\alpha - \epsilon = \sqrt{\eta}\mu_{\nu_x} + \epsilon$

$$\begin{aligned}
\int_{\theta-\sqrt{\eta}\alpha}^{\theta+\sqrt{\eta}\alpha} p_N(n)\, \mathrm{d}n &\leqslant \int_{\theta-\sqrt{\eta}\alpha}^{\infty} p_N(n)\, \mathrm{d}n \\
&\leqslant \int_{\theta-\sqrt{\eta}\alpha-\epsilon}^{\infty} p_N(n)\, \mathrm{d}n \\
&\leqslant \int_{\sqrt{\eta}\mu_{\nu_x}+\epsilon}^{\infty} p_N(n)\, \mathrm{d}n \\
&= \Pr\{N \geqslant \sqrt{\eta}\mu_{\nu_x} + \epsilon\} \\
&= \Pr\{N \geqslant \mu + \epsilon\} \\
&= \Pr\{N - \mu \geqslant \epsilon\} \\
&\leqslant \Pr\{|N - \mu| \geqslant \epsilon\} \\
&\leqslant \frac{\sigma^2}{\epsilon^2}.
\end{aligned}$$

So the conditional probability difference in (B.9) vanishes as $\sigma_{\nu_x}^2 \to 0$, as $r \to \infty$, as $\eta_E, \eta_B \to 1$, and as $G \to 1$ when $-\theta + \alpha < \mu_{\nu_x} < \theta - \alpha$ and with the constraint $\sqrt{\eta} \leqslant \min(\theta/|\mu_{\nu_x} + \alpha|, \theta/|\mu_{\nu_x} - \alpha|)$.

Case 3. Suppose next that $\mu_{\nu_x} > \theta + \alpha$ so that $\mu_{\nu_x} - \alpha > \theta > 0$. We first prove that the conditional probability difference in (B.8) vanishes as $\sigma_{\nu_x}^2 \to 0$, as $r \to \infty$, as $\eta_E, \eta_B \to 1$ and as $G \to 1$. So $\mu_{\nu_x} > -\theta + \alpha$ if $\mu_{\nu_x} > \theta + \alpha$. Thus $\mu_{\nu_x} > -\theta + \alpha$ and $\mu_{\nu_x} - \alpha > -\theta$ and $\sqrt{\eta}(\mu_{\nu_x} - \alpha) > -\theta$ for any $\sqrt{\eta} \geqslant 0$. Pick $\epsilon = \frac{1}{2}(\sqrt{\eta}\mu_{\nu_x} + \theta - \sqrt{\eta}\alpha) > 0$. So $-\theta + \sqrt{\eta}\alpha + \epsilon = \sqrt{\eta}\mu_{\nu_x} - \epsilon$. Then

$$\begin{aligned}
\int_{-\theta-\sqrt{\eta}\alpha}^{-\theta+\sqrt{\eta}\alpha} p_N(n)\,\mathrm{d}n &\leqslant \int_{-\infty}^{-\theta+\sqrt{\eta}\alpha} p_N(n)\,\mathrm{d}n \\
&\leqslant \int_{-\infty}^{-\theta+\sqrt{\eta}\alpha+\epsilon} p_N(n)\,\mathrm{d}n \\
&\leqslant \int_{-\infty}^{\sqrt{\eta}\mu_{\nu_x}-\epsilon} p_N(n)\,\mathrm{d}n \\
&= \Pr\{N \leqslant \sqrt{\eta}\mu_{\nu_x} - \epsilon\} \\
&= \Pr\{N \leqslant \mu - \epsilon\} \\
&= \Pr\{N - \mu \leqslant -\epsilon\} \\
&\leqslant \Pr\{|N - \mu| \geqslant \epsilon\} \\
&\leqslant \frac{\sigma^2}{\epsilon^2}.
\end{aligned}$$

So the conditional probability difference in (B.8) vanishes as $\sigma_{\nu_x}^2 \to 0$, as $r \to \infty$, as $\eta_E, \eta_B \to 1$, and as $G \to 1$ when $\mu_{\nu_x} > \theta + \alpha$. We prove last that the conditional probability difference in (B.9) vanishes as $\sigma_{\nu_x}^2 \to 0$, as $r \to \infty$, as $\eta_E, \eta_B \to 1$, and as $G \to 1$ when $\mu_{\nu_x} > \theta + \alpha$. So $\sqrt{\eta}(\mu_{\nu_x} - \alpha) > \theta$ whenever $\sqrt{\eta} > \theta/(\mu_{\nu_x} - \alpha)$. Pick $\epsilon = \frac{1}{2}(\sqrt{\eta}\mu_{\nu_x} - \theta - \sqrt{\eta}\alpha) > 0$. So $\theta + \sqrt{\eta}\alpha + \epsilon = \sqrt{\eta}\mu_{\nu_x} - \epsilon$. Then

$$\begin{aligned}
\int_{\theta-\sqrt{\eta}\alpha}^{\theta+\sqrt{\eta}\alpha} p_N(n)\,\mathrm{d}n &\leqslant \int_{-\infty}^{\theta+\sqrt{\eta}\alpha} p_N(n)\,\mathrm{d}n \\
&\leqslant \int_{-\infty}^{\theta+\sqrt{\eta}\alpha+\epsilon} p_N(n)\,\mathrm{d}n \\
&\leqslant \int_{-\infty}^{\sqrt{\eta}\mu_{\nu_x}-\epsilon} p_N(n)\,\mathrm{d}n \\
&= \Pr\{N \leqslant \sqrt{\eta}\mu_{\nu_x} - \epsilon\} \\
&= \Pr\{N \leqslant \mu - \epsilon\} \\
&= \Pr\{N - \mu \leqslant -\epsilon\} \\
&\leqslant \Pr\{|N - \mu| \geqslant \epsilon\} \\
&\leqslant \frac{\sigma^2}{\epsilon^2}.
\end{aligned}$$

So the conditional probability difference in (B.9) as $\sigma_{\nu_x}^2 \to 0$, as $r \to \infty$, and as $\eta_E, \eta_B \to 1$ when $\mu_{\nu_x} > \theta + \alpha$ and with the constraint $\sqrt{\eta} > \theta/(\mu_{\nu_x} - \alpha)$. Thus $\mu_{\nu_x} \notin (-\theta - \alpha, -\theta + \alpha) \cup (\theta - \alpha, \theta + \alpha)$ is a sufficient condition for the nonmonotone SR effect to occur with the given constraints on the product $\sqrt{\eta}$. □

Proof (Necessity). We prove that the SR effect does not occur when $\mu_{v_x} \in (-\theta - \alpha, -\theta + \alpha) \cup (\theta - \alpha, \theta + \alpha)$.

Case 1. Suppose first that $\mu_{v_x} \in (-\theta - \alpha, -\theta + \alpha)$. We prove with a similar Chebyshev bound that the conditional probabilities $p_{Y|S}(0|0) \to 1$ and $p_{Y|S}(\varepsilon|1) \to 1$ as $\sigma_{v_x}^2 \to 0$, as $r \to \infty$, as $\eta_E, \eta_B \to 1$, and as $G \to 1$. Then the mutual information $I(S,Y)$ approaches its maximum $H(S)$ as all noise vanish. Consider $p_{Y|S}(0|0)$. Pick any $\mu_{v_x} \in (-\theta - \alpha, -\theta + \alpha)$. Then $-\theta + \alpha > \mu_{v_x}$ and $\alpha - \mu_{v_x} > \theta$. Then $-\theta > \sqrt{\eta}(\mu_{v_x} - \alpha)$ whenever $\sqrt{\eta} > \theta/|\alpha - \mu_{v_x}|$. Pick $\epsilon = \frac{1}{2}(-\theta + \sqrt{\eta}\alpha - \sqrt{\eta}\mu_{v_x}) > 0$ so that $-\theta + \sqrt{\eta}\alpha - \epsilon = \sqrt{\eta}\mu_{v_x} + \epsilon$. Then

$$\begin{aligned}
p_{Y|S}(0|0) &= \int_{-\infty}^{-\theta+\sqrt{\eta}\alpha} p_N(n)\, \mathrm{d}n \\
&\geqslant \int_{-\infty}^{-\theta+\sqrt{\eta}\alpha-\epsilon} p_N(n)\, \mathrm{d}n \\
&= \int_{-\infty}^{\sqrt{\eta}\mu_{v_x}+\epsilon} p_N(n)\, \mathrm{d}n \\
&= 1 - \int_{\sqrt{\eta}\mu_{v_x}+\epsilon}^{\infty} p_N(n)\, \mathrm{d}n \\
&= 1 - \Pr\{N \geqslant \sqrt{\eta}\mu_{v_x} + \epsilon\} \\
&= 1 - \Pr\{N \geqslant \mu + \epsilon\} \\
&= 1 - \Pr\{N - \mu \geqslant \epsilon\} \\
&\geqslant 1 - \Pr\{|N - \mu| \geqslant \epsilon\} \\
&\geqslant 1 - \frac{\sigma^2}{\epsilon^2} \\
&\to 1
\end{aligned}$$

as $\sigma_{v_x}^2 \to 0$, as $r \to \infty$, as $\eta_E, \eta_B \to 1$, and as $G \to 1$. We prove the result similarly for $p_{Y|S}(\varepsilon|1)$. We show that $p_{Y|S}(0|1) \to 0$ and $p_{Y|S}(1|1) \to 0$ so that $p_{Y|S}(\varepsilon|1) \to 1$. Pick any $\mu_{v_x} \in (-\theta - \alpha, -\theta + \alpha)$. Then $\mu_{v_x} > -\theta - \alpha$ and $\mu_{v_x} + \alpha > -\theta$. $\sqrt{\eta}(\mu_{v_x} + \alpha) > -\theta$ and $\sqrt{\eta}\mu_{v_x} + \sqrt{\eta}\alpha + \theta > 0$ whenever $\sqrt{\eta} < \theta/|\mu_{v_x} + \alpha|$. Pick $\epsilon = \frac{1}{2}(\sqrt{\eta}\mu_{v_x} + \sqrt{\eta}\alpha + \theta) > 0$ so that $-\theta - \sqrt{\eta}\alpha + \epsilon = \sqrt{\eta}\mu_{v_x} - \epsilon$. Then

$$\begin{aligned}
p_{Y|S}(0|1) &= \int_{-\infty}^{-\theta-\sqrt{\eta}\alpha} p_N(n)\, \mathrm{d}n \\
&\leqslant \int_{-\infty}^{-\theta-\sqrt{\eta}\alpha+\epsilon} p_N(n)\, \mathrm{d}n \\
&= \int_{-\infty}^{\sqrt{\eta}\mu_{v_x}-\epsilon} p_N(n)\, \mathrm{d}n \\
&= \Pr\{N \leqslant \sqrt{\eta}\mu_{v_x} - \epsilon\} \\
&= \Pr\{N \leqslant \mu - \epsilon\} \\
&= \Pr\{N - \mu \leqslant -\epsilon\} \\
&\leqslant \Pr\{|N - \mu| \geqslant \epsilon\} \\
&\leqslant \frac{\sigma^2}{\epsilon^2}.
\end{aligned}$$

Pick any $\mu_{v_x} \in (-\theta - \alpha, -\theta + \alpha)$. Then $\mu_{v_x} < -\theta + \alpha$ and $\theta < \alpha - \mu_{v_x}$. $\sqrt{\eta G}(\mu_{v_x} - \alpha) < -\theta$ and $-\sqrt{\eta}\mu_{v_x} + \sqrt{\eta}\alpha - \theta > 0$ whenever $\sqrt{\eta} > \theta/|\alpha - \mu_{v_x}|$. Pick $\epsilon = \frac{1}{2}(-\sqrt{\eta}\mu_{v_x} + \sqrt{\eta}\alpha - \theta) > 0$

so that $-\theta + \sqrt{\eta}\alpha - \epsilon = \sqrt{\eta}\mu_{\nu_x} + \epsilon$. Then

$$\begin{aligned}
p_{Y|S}(1|1) &= \int_{\theta-\sqrt{\eta}\alpha}^{\infty} p_N(n)\,\mathrm{d}n \\
&\leqslant \int_{-\theta+\sqrt{\eta}\alpha}^{\infty} p_N(n)\,\mathrm{d}n \\
&\leqslant \int_{-\theta+\sqrt{\eta}\alpha-\epsilon}^{\infty} p_N(n)\,\mathrm{d}n \\
&= \int_{\sqrt{\eta}\mu_{\nu_x}+\epsilon}^{\infty} p_N(n)\,\mathrm{d}n \\
&= \Pr\{N \geqslant \sqrt{\eta}\mu_{\nu_x} + \epsilon\} \\
&= \Pr\{N \geqslant \mu + \epsilon\} \\
&= \Pr\{N - \mu \geqslant \epsilon\} \\
&\leqslant \Pr\{|N - \mu| \geqslant \epsilon\} \\
&\leqslant \frac{\sigma^2}{\epsilon^2}.
\end{aligned}$$

So $p_{Y|S}(\varepsilon|1) \to 1$ because $p_{Y|S}(0|1) \to 0$ and $p_{Y|S}(1|1) \to 0$ as $\sigma^2_{\nu_x} \to 0$, as $r \to \infty$, as $\eta_E, \eta_B \to 1$, and as $G \to 1$ and with constraint $\theta/|\alpha - \mu_{\nu_x}| < \sqrt{\eta} < \theta/|\alpha + \mu_{\nu_x}|$.

Case 2. Now suppose that $\mu_{\nu_x} \in (\theta - \alpha, \theta + \alpha)$. We prove that the conditional probabilities $p_{Y|S}(\varepsilon|0) \to 1$ and $p_{Y|S}(1|1) \to 1$ as $\sigma^2_{\nu_x} \to 0$, as $r \to \infty$, as $\eta_E, \eta_B \to 1$, and as $G \to 1$. We first prove that $p_{Y|S}(\varepsilon|0) \to 1$ in the limit of zero noise. We prove this by showing that $p_{Y|S}(0|0) \to 0$ and $p_{Y|S}(1|0) \to 0$ in the limit. Pick any $\mu_{\nu_x} \in (\theta - \alpha, \theta + \alpha)$. Then $\mu_{\nu_x} > \theta - \alpha$ and $\mu_{\nu_x} + \alpha > \theta$. $\sqrt{\eta}(\mu_{\nu_x} + \alpha) > \theta$ and $\sqrt{\eta}\mu_{\nu_x} + \sqrt{\eta}\alpha - \theta > 0$ whenever $\sqrt{\eta} > \theta/(\mu_{\nu_x} + \alpha)$. Pick $\epsilon = \frac{1}{2}(\sqrt{\eta}\mu_{\nu_x} + \sqrt{\eta}\alpha - \theta) > 0$ so that $\theta - \sqrt{\eta}\alpha + \epsilon = \sqrt{\eta}\mu_{\nu_x} - \epsilon$:

$$\begin{aligned}
p_{Y|S}(0|0) &= \int_{-\infty}^{-\theta+\sqrt{\eta}\alpha} p_N(n)\,\mathrm{d}n \\
&\leqslant \int_{-\infty}^{\theta-\sqrt{\eta}\alpha} p_N(n)\,\mathrm{d}n \\
&\leqslant \int_{-\infty}^{\theta-\sqrt{\eta}\alpha+\epsilon} p_N(n)\,\mathrm{d}n \\
&= \int_{-\infty}^{\sqrt{\eta}\mu_{\nu_x}-\epsilon} p_N(n)\,\mathrm{d}n \\
&= \Pr\{N \leqslant \sqrt{\eta}\mu_{\nu_x} - \epsilon\} \\
&= \Pr\{N \leqslant \mu - \epsilon\} \\
&= \Pr\{N - \mu \leqslant -\epsilon\} \\
&\leqslant \Pr\{|N - \mu| \geqslant \epsilon\} \\
&\leqslant \frac{\sigma^2}{\epsilon^2}.
\end{aligned}$$

Pick any $\mu_{\nu_x} \in (\theta - \alpha, \theta + \alpha)$. Then $\mu_{\nu_x} < \theta + \alpha$ and $\mu_{\nu_x} - \alpha < \theta$. $\sqrt{\eta}(\mu_{\nu_x} - \alpha) < \theta$ and $-\sqrt{\eta}\mu_{\nu_x} + \sqrt{\eta}\alpha + \theta > 0$ whenever $\sqrt{\eta} < \theta/|\mu_{\nu_x} - \alpha|$. Pick $\epsilon = \frac{1}{2}(-\sqrt{\eta}\mu_{\nu_x} + \sqrt{\eta}\alpha + \theta) > 0$ so that $\theta + \sqrt{\eta}\alpha - \epsilon = \sqrt{\eta}\mu_{\nu_x} + \epsilon$. Then

$$p_{Y|S}(1|0) = \int_{\theta+\sqrt{\eta}\alpha}^{\infty} p_N(n)\,\mathrm{d}n$$

$$
\begin{aligned}
&\leqslant \int_{\theta+\sqrt{\eta}\alpha-\epsilon}^{\infty} p_N(n)\,\mathrm{d}n \\
&= \int_{\sqrt{\eta}\mu_{v_x}+\epsilon}^{\infty} p_N(n)\,\mathrm{d}n \\
&= \Pr\{N \geqslant \sqrt{\eta}\mu_{v_x} + \epsilon\} \\
&= \Pr\{N \geqslant \mu + \epsilon\} \\
&= \Pr\{N - \mu \geqslant \epsilon\} \\
&\leqslant \Pr\{|N - \mu| \geqslant \epsilon\} \\
&\leqslant \frac{\sigma^2}{\epsilon^2}.
\end{aligned}
$$

So $p_{Y|S}(\varepsilon|0) \to 1$ because $p_{Y|S}(0|0) \to 0$ and $p_{Y|S}(1|0) \to 0$ as $\sigma_{v_x}^2 \to 0$, as $r \to \infty$, as $\eta_E, \eta_B \to 1$, and as $G \to 1$. Now we prove that $p_{Y|S}(1|1) \to 1$ as $\sigma_{v_x}^2 \to 0$, as $r \to \infty$, as $\eta_E, \eta_B \to 1$, and as $G \to 1$ whenever $\mu_{v_x} \in (\theta - \alpha, \theta + \alpha)$. Pick any $\mu_{v_x} \in (\theta - \alpha, \theta + \alpha)$. Then $\mu_{v_x} < \theta + \alpha$ and $\mu_{v_x} - \alpha < \theta$. $\sqrt{\eta}(\mu_{v_x} - \alpha) < \theta$ and $-\sqrt{\eta}\mu_{v_x} + \sqrt{\eta}\alpha + \theta > 0$ whenever $\sqrt{\eta} < \theta/|\mu_{v_x} - \alpha|$. Pick $\epsilon = \frac{1}{2}(-\sqrt{\eta}\mu_{v_x} + \sqrt{\eta}\alpha + \theta) > 0$ so that $\theta - \sqrt{\eta}\alpha + \epsilon = \sqrt{\eta}\mu_{v_x} - \epsilon$. Then

$$
\begin{aligned}
p_{Y|S}(1|1) &= \int_{\theta-\sqrt{\eta}\alpha}^{\infty} p_N(n)\,\mathrm{d}n \\
&\geqslant \int_{\theta-\sqrt{\eta}\alpha+\epsilon}^{\infty} p_N(n)\,\mathrm{d}n \\
&= \int_{\sqrt{\eta}\mu_{v_x}-\epsilon}^{\infty} p_N(n)\,\mathrm{d}n \\
&= 1 - \int_{-\infty}^{\sqrt{\eta}\mu_{v_x}-\epsilon} p_N(n)\,\mathrm{d}n \\
&= 1 - \Pr\{N \leqslant \sqrt{\eta}\mu_{v_x} - \epsilon\} \\
&= 1 - \Pr\{N \leqslant \mu - \epsilon\} \\
&= 1 - \Pr\{N - \mu \leqslant -\epsilon\} \\
&\geqslant 1 - \Pr\{|N - \mu| \geqslant \epsilon\} \\
&\geqslant 1 - \frac{\sigma^2}{\epsilon^2}.
\end{aligned}
$$

So $p_{Y|S}(1|1) \to 1$ as $\sigma_{v_x}^2 \to 0$, as $r \to \infty$, as $\eta_E, \eta_B \to 1$, and as $G \to 1$ whenever $\mu_{v_x} \in (\theta - \alpha, \theta + \alpha)$ and with constraint $\theta/(\mu_{v_x} + \alpha) < \sqrt{\eta} < \theta/|\mu_{v_x} - \alpha|$. The mutual information $I(S,Y)$ approaches its maximum $H(S)$ as all noises vanish. The SR effect does not occur for Alice's and Bob's mutual information whenever $\mu_{v_x} \in (-\theta-\alpha, -\theta+\alpha) \cup (\theta-\alpha, \theta+\alpha)$ with the above constraints on the product $\sqrt{\eta}$. □

Appendix B.2. Proof of theorem 4 (infinite variance)

The proof for sufficiency and necessity follows the same stable proof method with some modifications. We use the same characteristic function $\varphi_{v_x}(\omega)$ in (A.9) for alpha-stable random variable v_x. Suppose

$$
\sigma_{\mathcal{N}}^2 = \left(\eta_B \left(\begin{array}{c} \eta_E G e^{-2r} + \eta_E(G-1) \\ +\,(1-\eta_E) \end{array} \right) + 1 - \eta_B \right) \Big/ 2. \tag{B.10}
$$

The characteristic function $\varphi_N(\omega)$ of $p_N(n)$ is as follows:

$$\varphi_N(\omega) = \varphi_{v_x}(\sqrt{\eta}\omega) \exp\left\{-\frac{\sigma_N^2 \omega^2}{2}\right\} \tag{B.11}$$

from (5) and the convolution theorem.

Proof (Sufficiency). Take the limit of the characteristic function $\varphi_N(\omega)$ as $\gamma \to 0$, as $r \to \infty$, as $G \to 1$, and as $\eta_E, \eta_B \to 1$ to obtain the following characteristic function:

$$\lim_{\substack{r\to\infty,\gamma\to 0,\\ G\to 1,\eta_E,\eta_B\to 1}} \varphi_N(\omega) = \exp\{ia\omega\}. \tag{B.12}$$

The probability density $p_N(n)$ then approaches a translated delta function

$$\lim_{r\to\infty,\gamma\to 0,\eta_E,\eta_B\to 1} p_N(n) = \delta(n-a). \tag{B.13}$$

Suppose that $a \notin (-\theta-\alpha, -\theta+\alpha) \cup (\theta-\alpha, \theta+\alpha)$. Consider the case where $y = 0$. Then

$$\lim_{\substack{r\to\infty,\gamma\to 0,\\ G\to 1,\eta_E,\eta_B\to 1}} p_{Y|S}(0|0) - p_{Y|S}(0|1) \tag{B.14}$$

$$= \lim_{\substack{r\to\infty,\gamma\to 0,\\ G\to 1,\eta_E,\eta_B\to 1}} \int_{-\theta-\sqrt{\eta}\alpha}^{-\theta+\sqrt{\eta}\alpha} p_N(n)\, \mathrm{d}n \tag{B.15}$$

$$\to \int_{-\theta-\alpha}^{-\theta+\alpha} \delta(n-a)\, \mathrm{d}n = 0 \tag{B.16}$$

because $a \notin (-\theta-\alpha, -\theta+\alpha)$. Consider the case where $y = 1$:

$$\lim_{\substack{r\to\infty,\gamma\to 0,\\ G\to 1,\eta_E,\eta_B\to 1}} p_{Y|S}(1|1) - p_{Y|S}(1|0) \tag{B.17}$$

$$= \lim_{\substack{r\to\infty,\gamma\to 0,\\ G\to 1,\eta_E,\eta_B\to 1}} \int_{\theta-\sqrt{\eta}\alpha}^{\theta+\sqrt{\eta}\alpha} p_N(n)\, \mathrm{d}n \tag{B.18}$$

$$\to \int_{\theta-\alpha}^{\theta+\alpha} \delta(n-a)\, \mathrm{d}n = 0 \tag{B.19}$$

because $a \notin (\theta-\alpha, \theta+\alpha)$. □

Proof (Necessity). Suppose that $a \in (-\theta-\alpha, -\theta+\alpha) \cup (\theta-\alpha, \theta+\alpha)$.

Case 1. Pick $a \in (-\theta-\alpha, -\theta+\alpha)$. We show that $p_{Y|S}(0|0) \to 1$ and $p_{Y|S}(\varepsilon|1) \to 1$. Then

$$p_{Y|S}(0|0) = \int_{-\infty}^{-\theta+\sqrt{\eta}\alpha_x} p_N(n)\, \mathrm{d}n \tag{B.20}$$

$$= \int_{-\infty}^{-\theta} p_N(n+\sqrt{\eta}\alpha_x)\, \mathrm{d}n \tag{B.21}$$

$$\to \int_{-\infty}^{-\theta} \delta(n-a+\alpha)\, \mathrm{d}n \tag{B.22}$$

$$= \int_{-\infty}^{-\theta+\alpha} \delta(n-a)\, \mathrm{d}n = 1 \tag{B.23}$$

$$p_{Y|S}(\varepsilon|1) = \int_{-\theta-\sqrt{\eta}\alpha}^{\theta-\sqrt{\eta}\alpha} p_N(n)\,\mathrm{d}n \tag{B.24}$$

$$\to \int_{-\theta-\alpha}^{\theta-\alpha} \delta(n-a)\,\mathrm{d}n \tag{B.25}$$

$$= 1. \tag{B.26}$$

Case 2. Pick $a \in (\theta-\alpha, \theta+\alpha)$. We show that $p_{Y|S}(1|1) \to 1$ and $p_{Y|S}(\varepsilon|0) \to 1$. Then

$$p_{Y|S}(1|1) = \int_{\theta-\sqrt{\eta}\alpha}^{\infty} p_N(n)\,\mathrm{d}n \tag{B.27}$$

$$= \int_{\theta}^{\infty} p_N(n-\sqrt{\eta}\alpha_x)\,\mathrm{d}n \tag{B.28}$$

$$\to \int_{\theta}^{\infty} \delta(n-a-\alpha)\,\mathrm{d}n \tag{B.29}$$

$$= \int_{\theta-\alpha}^{\infty} \delta(n-a)\,\mathrm{d}n = 1. \tag{B.30}$$

$$p_{Y|S}(\varepsilon|0) = \int_{-\theta+\sqrt{\eta}\alpha}^{\theta+\sqrt{\eta}\alpha} p_N(n)\,\mathrm{d}n \tag{B.31}$$

$$\to \int_{-\theta+\alpha}^{\theta+\alpha} \delta(n-a)\,\mathrm{d}n \tag{B.32}$$

$$= 1. \tag{B.33}$$

□

References

[1] Benzi R, Sutera A and Vulpiani A 1981 The mechanism of stochastic resonance *J. Phys. A: Math. Gen.* **14** 453–7

[2] Wiesenfeld K and Moss F 1995 Stochastic resonance and the benefits of noise: from ice ages to crayfish and squids *Nature* **373** 33–6

[3] Bulsara A R and Gammaitoni L 1996 Tuning into noise *Phys. Today* **49** 39–45

[4] Gammaitoni L, Hänggi P, Jung P and Marchesoni F 1998 Stochastic resonance *Rev. Mod. Phys.* **70** 223–87

[5] Kosko B 2006 *Noise* (New York: Penguin)

[6] Patel A and Kosko B 2009 Optimal noise benefits in Neyman–Pearson and inequality-constrained statistical signal detection *IEEE Trans. Signal Process.* **57** 1655–69

[7] Goychuk I and Hänggi P 1999 Quantum stochastic resonance in parallel *New J. Phys.* **1**

[8] Bulsara A R and Zador A 1996 Threshold detection of wideband signals: a noise-induced maximum in the mutual information *Phys. Rev.* E **54** R2185–R2188

[9] Inchiosa M E, Robinson J W C and Bulsara A R 2000 Information-theoretic stochastic resonance in noise-floor limited systems: the case for adding noise *Phys. Rev. Lett.* **85** 3369–72

[10] Kosko B and Mitaim S 2003 Stochastic resonance in noisy threshold neurons *Neural Netw.* **14** 755–61

[11] Kosko B and Mitaim S 2004 Robust stochastic resonance for simple threshold neurons *Phys. Rev.* E **70** 031911

[12] Deco G and Schürmann B 1998 Stochastic resonance in the mutual information between input and output spike trains of noisy central neurons *Physica* D **117** 276–82

[13] Godivier X and Chapeau-Blondeau F 1998 Stochastic resonance in the information capacity of a nonlinear dynamic system *Int. J. Bifurcation Chaos* **8** 581–9

[14] Inchiosa M E, Robinson J W C and Bulsara A R 2000 Information-theoretic stochastic resonance in noise-floor limited systems: the case for adding noise *Phys. Rev. Lett.* **85** 3369–72

[15] Mitaim S and Kosko B 2004 Adaptive stochastic resonance in noisy neurons based on mutual information *IEEE Trans. Neural Netw.* **15** 1526–40
[16] Patel A and Kosko B 2009 Error-probability noise benefits in threshold neural signal detection *Neural Netw.* **22** 697–706
[17] Patel A and Kosko B 2008 Stochastic resonance in continuous and spiking neuron models with levy noise *IEEE Trans. Neural Netw.* **19** 1993–2008
[18] Kosko B and Mitaim S 2001 Robust stochastic resonance: signal detection and adaptation in impulsive noise *Phys. Rev.* E **64** 051110
[19] Mitaim S and Kosko B 1998 Adaptive stochastic resonance *Proc. IEEE: Special Issue on Intell. Signal Process.* **86** 2152–83
[20] Loudon R and Knight P L 1987 Squeezed light *Modern Opt.* **34** 709–59
[21] Gerry C C and Knight P L 2005 *Introductory Quantum Optics* (Cambridge: Cambridge University Press)
[22] Hirano T, Konishi T and Namiki R 2000 Quantum cryptography using balanced homodyne detection arXiv:quant-ph/0008037
[23] Namiki R and Hirano T 2003 Security of quantum cryptography using balanced homodyne detection *Phys. Rev.* A **67** 022308
[24] Holevo A S and Werner R F 2001 Evaluating capacities of bosonic Gaussian channels *Phys. Rev.* A **63** 032312
[25] Cover T M and Thomas J A 1991 *Elements of Information Theory* (New York: Wiley)
[26] Leonhardt U and Paul H 1993 Realistic optical homodyne measurements and quasiprobability distributions *Phys. Rev.* A **48** 4598–604
[27] Hall M J W 1994 Gaussian noise and quantum-optical communication *Phys. Rev.* A **50** 3295–303
[28] Glauber R J 2005 *One Hundred Years of Light Quanta Les Prix Nobel. The Nobel Prizes 2005* ed K Grandin (Stockholm: Nobel Foundation) pp 90–1
[29] Breiman L 1968 *Probability* (Reading, MA: Addison-Wesley)
[30] Nikias C L and Shao M 1995 *Signal Processing with Alpha-Stable Distributions and Applications* (New York: Wiley)
[31] Bennett C H and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing *Proc. of IEEE Int. Conf. on Computers Systems and Signal Processing (Bangalore, India, December 1984)* pp 175–9
[32] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dusek M, Lutkenhaus N and Peev M 2008 The security of practical quantum key distribution arXiv:0802.4155
[33] Namiki R and Hirano T 2005 Security of continuous-variable quantum cryptography using coherent states: decline of postselection advantage *Phys. Rev.* A **72** 024301
[34] Haus H A and Mullen J A 1962 Quantum noise in linear amplifiers *Phys. Rev.* **128** 2407–13
[35] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)
[36] Renner R, Gisin N and Kraus B 2005 Information-theoretic security proof for quantum-key-distribution protocols *Phys. Rev.* A **72** 012332
[37] Devetak I 2005 The private classical capacity and quantum capacity of a quantum channel *IEEE Trans. Inf. Theory* **51** 44–55