Defeating passive eavesdropping with quantum illumination

Defeating passive eavesdropping with quantum illumination

Jeffrey H. Shapiro*

Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA

(Received 18 March 2009; published 17 August 2009)

A two-way protocol for defeating passive eavesdropping is proposed. For each information bit, Alice sends Bob T sec of signal-beam output from a spontaneous parametric down-converter over a pure-loss channel while retaining the idler beam with which it is maximally entangled. Bob imposes a single information bit on the light he receives from Alice via binary phase-shift keying. He then amplifies the modulated beam and sends the resulting light back to Alice over the same pure-loss channel. Even though the loss and amplifier noise destroy any entanglement between the light that Alice receives from Bob and the idler she has retained, she can decode Bob's bit with an error probability that can be orders of magnitude lower than what is achieved by a passive eavesdropper who receives all the photons that are lost en route from Alice to Bob and from Bob to Alice. In particular, Alice and Bob can communicate at 50 Mbit/s over 50 km of low-loss fiber with an error probability of less than 10^{-6} while the passive eavesdropper's error probability must exceed 0.28.

DOI: 10.1103/PhysRevA.80.022320 PACS number(s): 03.67.Hk, 03.67.Mn, 42.50.Dv

The use of quantum key distribution (QKD) to ensure the security of classical information transmission has moved from its theoretical roots [1–3] to a major network demonstration [4]. The objective of QKD is for two geographically separated users—Alice and Bob—to create a shared set of completely random key bits in a manner that precludes an eavesdropper (Eve) from having anything more than an inconsequentially small amount of information about the entire set of key bits. That such a goal is possible arises from a fundamental quantum mechanical principle: Eve cannot tap the Alice-to-Bob channel without creating a disturbance on that channel. By ascribing all errors encountered to Eve's intrusion, Alice and Bob can either abort their QKD protocol—if this intrusion is too severe—or distill a final key about which Eve has a vanishingly small amount of information. QKD, however, is extremely lossy. In recent work [5], the Bennett-Brassard 1984 (BB84) protocol with a gigahertz transmitter pulse rate led to a distilled key rate of ~250 kbit/s over a 50-km-long fiber. So, although QKD systems can provide shared secret bits, they do not themselves afford a viable means for transmitting the random bit stream derived from source coding (lossless data compression) of an information-bearing message to its Shannon limit [6]. Indeed, for the 50 km system from [5], only ~0.4% of the transmitted bits were detected, and ~3% of them were received in error.

In this paper we present an optical communication protocol that defeats *passive* eavesdropping, in which Eve merely listens to Alice and Bob's transmissions. Our system is vulnerable to *active* attacks, in which Eve injects her own light to probe Alice and Bob's communication apparatus. Nevertheless, the enormous disparity between the bit error probabilities of a passive eavesdropper and the intended receiver make this scheme attractive for unencrypted information transmission when active attacks can be ruled out. In particular, unlike the BB84 protocol, our scheme *is* capable of high data rate, low error-probability transmission of the random bit stream derived from source coding of an information-bearing message.

The basis for our protocol is quantum illumination, specifically the Gaussian-state radar system described in [7]. There, the entangled signal and idler outputs from spontaneous parametric down conversion (SPDC) were shown to afford a substantial error-probability advantage—over a coherent-state system of the same average transmitted photon number—when the signal beam is used to irradiate a target region containing a bright thermal-noise bath in which a low-reflectivity object might be embedded, and the idler beam is retained at the transmitter for use in an optimal joint measurement with the light returned from the target region. This performance advantage is surprising because the loss and noise combine to destroy any entanglement between the return light and the retained idler. The origin of this advantage is the stronger-than-classical phase-sensitive cross correlation between the signal and idler produced by SPDC. When the source is operated in the low-brightness regime, this leads to a phase-sensitive cross correlation between the target return and the retained idler that outstrips any such correlation produced by a classical-state transmitter of the same average transmitted photon number [7]. Here, we will turn that capability to the task of secure communication between Alice and Bob in the presence of a passive eavesdropper Eve.

The communication system of interest is a two-way protocol. Alice transmits a light beam to Bob, who modulates and amplifies the light he receives, and then sends it back to Alice for detection. To exploit the quantum illumination paradigm, Alice uses a continuous-wave (cw) SPDC source, transmitting her signal beam to Bob while retaining (without loss) her idler beam for subsequent joint measurement with what she will receive from Bob. Each T-sec-long transmission from Alice comprises $M = WT \gg 1$ signal-idler mode pairs—where W is the source's phase-matching bandwidth—with annihilation operators $\{\hat{a}_{S_m}, \hat{a}_{I_m} : 1 \le m \le M\}$. Their joint density operator $\hat{\boldsymbol{\rho}}_{SI}$ is the tensor product of independent, identically distributed (iid) density operators for each mode pair that are zero-mean, jointly Gaussian states with the common Wigner-distribution covariance matrix

[*] jhs@mit.edu

$$\boldsymbol{\Lambda}_{SI} = \frac{1}{4}\begin{bmatrix} S & 0 & C_q & 0 \\ 0 & S & 0 & -C_q \\ C_q & 0 & S & 0 \\ 0 & -C_q & 0 & S \end{bmatrix}, \tag{1}$$

where $S \equiv 2N_S+1$ and $C_q \equiv 2\sqrt{N_S(N_S+1)}$, and N_S is the average photon number of each signal (and idler) mode [8]. Alice-to-Bob transmission occurs over a pure-loss channel [9]. Hence Bob receives a light beam whose modal annihilation operators are

$$\hat{a}_{B_m} = \sqrt{\kappa}\hat{a}_{S_m} + \sqrt{1-\kappa}\hat{e}_{B_m}, \quad \text{for } 1 \le m \le M, \tag{2}$$

where the environmental modes, $\{\hat{e}_{B_m}\}$, are in their vacuum states [10]. Bob first imposes a binary phase-shift keyed (BPSK) information bit (k=0 or 1) on the light he has received. He then employs a phase-insensitive amplifier with gain G, and transmits the amplified modulated light, with modal annihilation operators

$$\hat{a}'_{B_m} \equiv (-1)^k\sqrt{G}\hat{a}_{B_M} + \sqrt{G-1}\hat{a}^\dagger_{N_m}, \quad \text{for } 1 \le m \le M, \tag{3}$$

back to Alice through the same pure-loss channel. Here the $\{\hat{a}_{N_m}\}$ are in iid thermal states with $\langle \hat{a}_{N_m}\hat{a}^\dagger_{N_m}\rangle = N_B/(G-1) \ge 1$. Alice thus receives a light beam whose modal annihilation operators are

$$\hat{a}_{R_m} = \sqrt{\kappa}\hat{a}'_{B_m} + \sqrt{1-\kappa}\hat{e}_{A_m}, \quad \text{for } 1 \le m \le M, \tag{4}$$

where the $\{\hat{e}_{A_m}\}$ are in their vacuum states. Given Bob's information bit k, we have that $\hat{\boldsymbol{\rho}}^{(k)}_{RI}$, the joint state of Alice's $\{\hat{a}_{R_m}, \hat{a}_{I_m}\}$ modes, is the tensor product of iid, zero-mean, jointly Gaussian states for each mode pair with the common Wigner-distribution covariance matrix

$$\boldsymbol{\Lambda}^{(k)}_{RI} = \frac{1}{4}\begin{bmatrix} A & 0 & (-1)^k C_a & 0 \\ 0 & A & 0 & (-1)^{k+1} C_a \\ (-1)^k C_a & 0 & S & 0 \\ 0 & (-1)^{k+1} C_a & 0 & S \end{bmatrix}, \tag{5}$$

where $A \equiv 2\kappa^2 G N_S + 2\kappa N_B + 1$ and $C_a \equiv \kappa\sqrt{G}C_q$ [11]. Alice's task is to decode Bob's bit, which is equally likely to be k =0 or k=1, with minimum error probability.

Eve will be assumed to collect *all* the photons that are lost en route from Alice to Bob and from Bob to Alice [12], i.e., she has at her disposal the mode pairs $\{\hat{c}_{S_m}, \hat{c}_{R_m} : 1 \le m \le M\}$, where

$$\hat{c}_{S_m} = \sqrt{1-\kappa}\hat{a}_{S_m} - \sqrt{\kappa}\hat{e}_{B_m}, \tag{6}$$

$$\hat{c}_{R_m} = \sqrt{1-\kappa}\hat{a}'_{B_m} - \sqrt{\kappa}\hat{e}_{A_m}. \tag{7}$$

Given Bob's bit value, Eve's joint density operator, $\hat{\boldsymbol{\rho}}^{(k)}_{c_S c_R}$, is the tensor product of M iid mode-pair density operators that are zero-mean, jointly Gaussian states with the common Wigner-distribution covariance matrix

$$\boldsymbol{\Lambda}^{(k)}_{c_S c_R} = \frac{1}{4}\begin{bmatrix} D & 0 & (-1)^k C_e & 0 \\ 0 & D & 0 & (-1)^k C_e \\ (-1)^k C_e & 0 & E & 0 \\ 0 & (-1)^k C_e & 0 & E \end{bmatrix}, \tag{8}$$

where $D \equiv 2(1-\kappa)N_S+1$, $C_e \equiv 2(1-\kappa)\sqrt{\kappa G}N_S$, and $E \equiv 2(1-\kappa)\kappa G N_S + 2(1-\kappa)N_B + 1$. Eve too is interested in minimum error-probability decoding of Bob's bit.

Alice's minimum error-probability decision rule is to measure $\hat{\boldsymbol{\rho}}^{(1)}_{RI} - \hat{\boldsymbol{\rho}}^{(0)}_{RI}$, and declare that k=1 was sent if and only if her measurement outcome is non-negative. Similarly, Eve's minimum error-probability decision rule is to measure $\hat{\boldsymbol{\rho}}^{(1)}_{c_S c_R} - \hat{\boldsymbol{\rho}}^{(0)}_{c_S c_R}$ and declare that k=1 was sent if and only if her measurement outcome is non-negative. The exact error probabilities for these Gaussian-state hypothesis tests are not easy to evaluate. Thus, as in [7], we shall rely on quantum Chernoff bounds [13], which are known to be exponentially tight for iid M mode-pair problems, i.e., with

$$\Pr(e) \le e^{-M \max_{0 \le s \le 1} \mathcal{E}(s)}/2, \tag{9}$$

for

$$\mathcal{E}(s) \equiv -\ln(\mathrm{tr}[(\hat{\rho}^{(0)}_m)^s(\hat{\rho}^{(1)}_m)^{1-s}]), \tag{10}$$

giving the Chernoff bound (in terms of the conditional mode-pair density operators $\hat{\rho}^{(k)}_m$) on the exact error probability, we have

$$\lim_{M\to\infty} -\ln[2\Pr(e)]/M = \max_{0 \le s \le 1} \mathcal{E}(s). \tag{11}$$

The BPSK symmetry in $\hat{\boldsymbol{\rho}}^{(k)}_{RI}$ and $\hat{\boldsymbol{\rho}}^{(k)}_{c_S c_R}$ implies that s=1/2 optimizes the Chernoff bound exponents for both Alice and Eve. The following lower bound on the error probability of any receiver [7] will also be of use,

$$\Pr(e) \ge \frac{1-\sqrt{1-e^{-2M\mathcal{E}(1/2)}}}{2}; \tag{12}$$

it is not exponentially tight for the problems at hand.

Because all our conditional density operators are zero-mean Gaussian states, we can use the results of [14] to evaluate $\mathcal{E}(1/2)$ for Alice and Eve's receivers. To do so we need the symplectic diagonalizations of their conditional Wigner-distribution covariance matrices. The symplectic diagonalization of a 4×4 dimensional covariance matrix $\boldsymbol{\Lambda}$ consists of a 4×4 dimensional symplectic matrix $\boldsymbol{S}$ and a symplectic spectrum $\{\nu_n : 1 \le n \le 2\}$ that satisfy

$$\boldsymbol{S}\boldsymbol{\Omega}\boldsymbol{S}^T = \boldsymbol{\Omega} \equiv \begin{bmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{bmatrix}, \tag{13}$$

$$\boldsymbol{\Lambda} = \boldsymbol{S}\,\mathrm{diag}(\nu_1, \nu_1, \nu_2, \nu_2)\boldsymbol{S}^T, \tag{14}$$

where diag $(\cdot,\cdot,\cdot,\cdot)$ denotes a diagonal matrix with the given diagonal elements.

For our quantum-illumination (Alice-to-Bob-to-Alice)

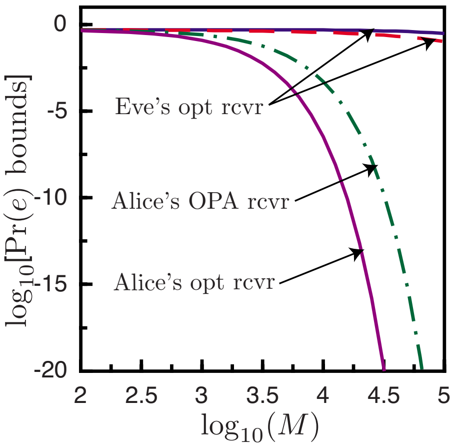

FIG. 1. (Color online) Error-probability bounds for $N_S=0.004$, $\kappa=0.1$, and $G=N_B=10^4$. Solid curves: Chernoff bounds for Alice and Eve's optimum quantum receivers. Dashed curve: error-probability lower bound for Eve's optimum quantum receiver. Dot-dashed curve: Bhattacharyya bound for Alice's OPA receiver.

communication, the symplectic matrices needed for the diagonalization of $\mathbf{\Lambda}_{RI}^{(k)}$ are

$$S^{(k)} = \begin{bmatrix} \mathbf{X}_+ & (-1)^k\mathbf{X}_- \\ (-1)^k\mathbf{X}_- & \mathbf{X}_+ \end{bmatrix}, \qquad (15)$$

for $k=0,1$. Here, $\mathbf{X}_\pm \equiv \text{diag}(x_\pm, \pm x_\pm)$ with

$$x_\pm \equiv \sqrt{\frac{A+S \pm \sqrt{(A+S)^2-4C_a^2}}{2\sqrt{(A+S)^2-4C_a^2}}}. \qquad (16)$$

The associated symplectic spectra are identical for $k=0$ and 1, i.e., for $n=1,2$ we have

$$\nu_n^{(k)} = [(-1)^n(S-A) + \sqrt{(A+S)^2-4C_a^2}]/8. \qquad (17)$$

For Eve's attempt to listen in, the symplectic matrices needed for the diagonalization of $\mathbf{\Lambda}_{c_Sc_R}^{(k)}$ are

$$S^{(k)} = \begin{bmatrix} \mathbf{Y} & (-1)^{k+1}\mathbf{Z} \\ (-1)^k\mathbf{Z} & \mathbf{Y} \end{bmatrix}, \qquad (18)$$

for $k=0,1$. Here, $\mathbf{Y} \equiv \text{diag}(\cos(\theta),\cos(\theta))$ and $\mathbf{Z} \equiv \text{diag}(\sin(\theta),\sin(\theta))$ with

$$\cos(2\theta) = \frac{D-E}{\sqrt{(D-E)^2+4C_e^2}}. \qquad (19)$$

The associated symplectic spectra are identical for $k=0$ and 1, i.e., for $n=1,2$ we have

$$\nu_n^{(k)} = [(D+E) - (-1)^n\sqrt{(D-E)^2+4C_e^2}]/8. \qquad (20)$$

The preceding diagonalizations lead to Chernoff bound expressions that are far too long to exhibit here. In Fig. 1 we compare the Chernoff bounds for Alice and Eve's optimum quantum receivers when $\kappa=0.1$, $N_S=0.004$, and $G=N_B=10^4$. Also included in this figure is the error-probability lower bound from Eq. (12) on Eve's optimum quantum receiver. We see that Alice's error probability *upper* bound—at a given M value—can be orders of magnitude lower than Eve's error-probability *lower* bound when both use optimum quantum reception. This occurs despite Eve's getting nine times more of Alice's transmission than Bob does and nine times more of Bob's transmission than Alice does. Note that Alice's performance advantage may be better assessed from comparing her error-probability upper bound with that of Eve's receiver, in that both are exponentially tight Chernoff bounds.

To show that the advantage afforded by quantum illumination extends well beyond the specific example chosen for Fig. 1, we have used an algebraic computation program to obtain the following approximate forms for the Chernoff bounds on the error probabilities of Alice and Eve's optimum quantum receivers:

$$\Pr(e)_{\text{Alice}} \le \frac{\exp(-4M\kappa G N_S/N_B)}{2}, \qquad (21)$$

$$\Pr(e)_{\text{Eve}} \le \frac{\exp(-4M\kappa(1-\kappa)G N_S^2/N_B)}{2}, \qquad (22)$$

which apply in the low-brightness, high-noise regime, viz., when $N_S \ll 1$ and $\kappa N_B \gg 1$. We see that Alice's Chernoff bound error exponent will be orders of magnitude *higher* than that of Eve in this regime, because

$$\mathcal{E}_{\text{Alice}}(1/2)/\mathcal{E}_{\text{Eve}}(1/2) = 1/(1-\kappa)N_s \gg 1. \qquad (23)$$

Thus the advantageous quantum illumination behavior shown in Fig. 1 is typical for this regime.

As yet we have not identified specific implementations for Alice or Eve's optimum quantum receivers. So, while we will accord Eve an optimum quantum receiver, let us show that Alice can still enjoy an enormous advantage in error probability when she uses a version of Guha's optical parametric amplifier (OPA) receiver for the quantum-illumination radar [15]. Here Alice uses an OPA to obtain a light beam whose modal annihilation operators are given by

$$\hat{a}_m' \equiv \sqrt{G_{\text{OPA}}}\hat{a}_{I_m} + \sqrt{G_{\text{OPA}}-1}\hat{a}_{R_m}^\dagger, \quad \text{for } 1 \le m \le M, \qquad (24)$$

where $G_{\text{OPA}} = 1 + N_S/\sqrt{\kappa N_B}$. She then makes a minimum error-probability decision based on the results of the photon-counting measurement $\Sigma_{m=1}^M \hat{a}_m'^\dagger \hat{a}_m'$ [16]. The Bhattacharyya bound [17] on this receiver's error probability in the $N_S \ll 1$, $\kappa N_B \gg 1$ regime turns out to be

$$\Pr(e)_{\text{OPA}} \le \frac{\exp(-2M\kappa N_S/N_B)}{2}, \qquad (25)$$

which is only 3dB inferior, in error exponent, to Alice's optimum quantum receiver. We have included the numerically evaluated Bhattacharyya bound for Alice's OPA receiver in Fig. 1, for the case $N_S=0.004$, $\kappa=0.1$, and $G=N_B=10^4$.

Some additional points are worth noting. BPSK communication is intrinsically phase sensitive, so Alice's receiver will require phase coherence that must be established through a tracking system. More importantly, there is the path-length versus bit-rate tradeoff. Operation must occur in the low-brightness regime. So, as channel loss increases, Alice must increase her mode-pair number M at constant N_S and G to maintain a sufficiently low error probability *and* immunity to passive eavesdropping. For a T-sec-long bit interval and W Hz SPDC phase-matching bandwidth, $M=WT$ implies that her bit rate will go down as loss increases at constant error probability. With $W=1$ THz and $T=20$ ns, so that $M=2\times 10^4$, the case shown in Fig. 1 will yield 50 Mbit/s communication with

$$\Pr(e)_{\mathrm{OPA}} \leq 5.09 \times 10^{-7} \tag{26}$$

and

$$0.285 \leq \Pr(e)_{\mathrm{Eve}} \leq 0.451 \tag{27}$$

when Alice and Bob are linked by 50 km of 0.2 dB/km loss fiber, assuming that the rest of their equipment is ideal. In fact, almost all of the equipment needed for realizing this performance is within reach of available technology. Commercial modulators and erbium-doped fiber amplifiers can fulfill Bob's needs. It is Alice who faces the more difficult equipment requirements. However, the periodically poled magnesium-oxide-doped lithium niobate (PP-MgO:LN) down-converter employed in [18] has a 17 THz phase-matching bandwidth and is capable of $N_S=0.004$ with 250 mW of cw pump power. Likewise, the PP-MgO:LN OPA employed in that same work can achieve $G_{\mathrm{OPA}}-1=0.00013$—the gain value needed for $N_S=0.004$, $\kappa=0.1$, and $N_B=10^4$—with only 8 mW of cw pump power. Furthermore, Alice's OPA receiver does not require single-photon sensitivity. The average number of photons impinging on her photodetector under the two bit-value possibilities are $\bar{N}_k=2.90\times 10^3$ for $k=0$, and 2.33×10^3 for $k=1$, implying that Alice may approach the photon-counting performance assumed in our analysis with a high quantum efficiency linear-mode avalanche photodiode. There is, however, one major technical difficulty Alice must face: lossless storage of her idler beam. Any loss in idler storage will degrade Alice's error-probability advantage over the ideal Eve. That loss of error-probability advantage could be ameliorated by a more realistic assessment of Eve's capabilities. In particular, is it reasonable to assume that a passive eavesdropper can collect all of Alice's light that does not reach Bob *and* all of Bob's light that does not reach Alice? For a free-space optical link, it should be easy to verify that Eve can only collect a fraction of the light that does not reach its intended destination. With optical time-domain reflectometry on a fiber link, it should be possible to estimate localized propagation losses that should be ascribed to an eavesdropper.

In conclusion, we have shown that quantum illumination can provide immunity to *passive* eavesdropping in a lossy, noisy environment despite that environment's destroying the entanglement produced by the source. To ward off active attacks, Alice and Bob must take measures to detect and defeat Eve's use of impersonation attacks, man-in-the-middle attacks, and optical probing of Bob's BPSK modulator. These attacks might be identified and dealt with if Alice and Bob employ authentication, monitor the physical integrity of the communication channel, check the received power level and its frequency spectrum at Bob's station, and verify the error probability at Alice's station.

This research was supported by the Office of Naval Research Basic Research Challenge Program, the W. M. Keck Foundation Center for Extreme Quantum Information Theory, and the DARPA Quantum Sensors Program.

[1] C. H. Bennett and G. Brassard, *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, India (IEEE, New York, 1984) p. 175.

[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

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

[4] SECOQC, Development of a Global Network for Secure Communication based on Quantum Cryptography, http://www.secoqc.net

[5] A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, Opt. Express **16**, 18790 (2008).

[6] R. G. Gallager, *Information Theory and Reliable Communication* (Wiley, New York, 1968), Chap. 3.

[7] S.-H. Tan, B. I. Erkmen, V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, S. Pirandola, and J. H. Shapiro, Phys. Rev. Lett. **101**, 253601 (2008).

[8] This state has maximum quadrature entanglement for its average photon number. Its closest classical-state counterpart is the zero-mean, jointly Gaussian state whose Wigner-distribution covariance is given by Eq. (1) with C_q replaced by $C_c\equiv 2N_S$. For low-brightness operation, wherein $N_S\ll 1$ prevails, we have $C_q\gg C_c$.

[9] V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, J. H. Shapiro, and H. P. Yuen, Phys. Rev. Lett. **92**, 027902 (2004).

[10] At near infrared through ultraviolet wavelengths, background light will be sufficiently weak that it can be ignored. For example, a typical daytime spectral radiance value of 10 W/m^2 sr μm at 1.55 μm wavelength [N. S. Kopeika and J. Bordogna, Proc. IEEE **58**, 1571 (1970)] leads to $\langle \hat{e}_{B_m}^{\dagger}\hat{e}_{B_m}\rangle \sim 10^{-6}$ for a line-of-sight terrestrial link; nighttime values are orders of magnitude lower. Room-temperature thermal noise is even weaker, viz., $\langle \hat{e}_{B_m}^{\dagger}\hat{e}_{B_m}\rangle \approx 4\times 10^{-14}$ at 1.55 μm wavelength for a 300 K noise temperature. Thus, our pure-loss (noiseless) channel model will suffice so long as $N_S\gg 10^{-6}$.

[11] For $N_B\geq \kappa G$, this state is *classical*, i.e., it has a proper P representation, hence it is *not* entangled.

[12] This assumption maximizes the information gained by a passive eavesdropper. The error probability disparity—between Alice and Eve's receivers—will only *increase* if Eve's coupling to either Alice or Bob's transmission is reduced from its theoretical maximum.

[13] K. M. R. Audenaert, J. Calsamiglia, R. Muñoz-Tapia, E. Bagan, Ll. Masanes, A. Acin, and F. Verstraete, Phys. Rev. Lett. **98**, 160501 (2007); J. Calsamiglia, R. Muñoz-Tapia, Ll. Masanes, A. Acin, and E. Bagan, Phys. Rev. A **77**, 032311 (2008).

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

[15] S. Guha, *Proceedings of IEEE International Symposium on Information Theory*, Seoul, Korea (IEEE, New York, 2009).

[16] Our use of modal representations to describe OPA operation and the subsequent photon-counting measurement does *not* imply that separate amplifiers are required for each mode pair nor that a separate photon-counting measurement must be made for each output mode. A cw-pumped OPA can be used to perform the desired operation on the return and idler beams, and one photodetector can be used to obtain the total photon count. These results follow immediately from modal expansions for the relevant positive-frequency field operators. For example, with $\hat{E}(t) \equiv \Sigma_m \hat{a}'_m e^{-j\omega_m t}/\sqrt{T}$ representing the positive-frequency field operator for a single T-sec-long bit interval at the OPA's output, our OPA receiver only needs to measure the total photon-count operator $\int dt \hat{E}^\dagger(t)\hat{E}(t)$.

[17] The Bhattacharyya bound is the Chernoff bound with $s=1/2$ used even when it is not the optimum choice.

[18] J. Le Gouët, D. Venkatraman, F. N. C. Wong, and J. H. Shapiro, *Postdeadline Paper Digest, International Quantum Electronics Conference*, Baltimore, MD (Optical Society of America, Washington, DC, 2009).