Defeating passive eavesdropping with quantum illumination

The MIT Faculty has made this article openly available. Please share how this access benefits you. Your story matters.

<table>
<thead>
<tr>
<th>Citation</th>
<th>Shapiro, Jeffrey H. “Defeating passive eavesdropping with quantum illumination.” Physical Review A 80.2 (2009): 022320. (C) 2010 The American Physical Society.</th>
</tr>
</thead>
<tbody>
<tr>
<td>As Published</td>
<td><a href="http://dx.doi.org/10.1103/PhysRevA.80.022320">http://dx.doi.org/10.1103/PhysRevA.80.022320</a></td>
</tr>
<tr>
<td>Publisher</td>
<td>American Physical Society</td>
</tr>
<tr>
<td>Version</td>
<td>Final published version</td>
</tr>
<tr>
<td>Accessed</td>
<td>Sun Dec 09 08:36:34 EST 2018</td>
</tr>
<tr>
<td>Citable Link</td>
<td><a href="http://hdl.handle.net/1721.1/51048">http://hdl.handle.net/1721.1/51048</a></td>
</tr>
<tr>
<td>Terms of Use</td>
<td>Article is made available in accordance with the publisher's policy and may be subject to US copyright law. Please refer to the publisher's site for terms of use.</td>
</tr>
<tr>
<td>Detailed Terms</td>
<td></td>
</tr>
</tbody>
</table>
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 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 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 $M = WT > 1$ signal-idler mode pairs—where $W$ is the source’s phase-matching bandwidth—with annihilation operators $\{a_s, a_i^\dagger \}_{1 ≤ m ≤ M}$. Their joint density operator $\hat{\rho}_S$ 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 $\hat{\rho}_S$.
\[ \Lambda_{sl} = \frac{1}{4} \begin{bmatrix} S & 0 & C_q & 0 \\ 0 & S & 0 & -C_q \\ C_q & 0 & S & 0 \\ 0 & -C_q & 0 & S \end{bmatrix}, \] (1)

where \( S = 2N_x + 1 \) and \( C_q = 2\sqrt{N_x(N_x+1)} \), and \( N_x \) 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

\[ \hat{a}_{B_m} = \sqrt{\kappa} \hat{a}_{S_m} + \sqrt{1 - \kappa} \hat{e}_{B_m}, \quad \text{for} \quad 1 \leq m \leq M, \] (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 \( (k=0 \text{ or } 1) \) 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

\[ \hat{a}_{B_m}^\prime = (-1)^k \sqrt{G} \hat{a}_{B_m} + \sqrt{G - 1} \hat{a}_{N_m}^\prime, \quad \text{for} \quad 1 \leq m \leq M, \] (3)

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

\[ \hat{a}_{N_m} = \sqrt{\kappa} \hat{a}_{S_m}^\prime + \sqrt{1 - \kappa} \hat{e}_{A_m}, \quad \text{for} \quad 1 \leq m \leq M, \] (4)

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

\[ \Lambda_{sl}^{(k)} = \frac{1}{4} \begin{bmatrix} A & 0 & (-1)^kC_a & 0 \\ 0 & A & 0 & (-1)^kC_a \\ (-1)^kC_a & 0 & S & 0 \\ 0 & (-1)^kC_a & 0 & S \end{bmatrix}, \] (5)

where \( A = 2\kappa^2G^2 + 2\kappa N_y + 1 \) and \( C_a = \kappa \sqrt{GC_y} \) [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 \( \{ \hat{e}_{S_m}, \hat{e}_{R_m} \}, 1 \leq m \leq M \}, \) where

\[ \hat{e}_{S_m} = \sqrt{1 - \kappa} \hat{a}_{S_m} - \sqrt{\kappa} \hat{e}_{B_m}, \] (6)

\[ \hat{e}_{R_m} = \sqrt{1 - \kappa} \hat{a}_{B_m} - \sqrt{\kappa} \hat{e}_{A_m}. \] (7)

Given Bob’s bit value, Eve’s joint density operator, \( \hat{\rho}^{(k)}_{sr} \), 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

\[ \Lambda_{sr}^{(k)} = \frac{1}{4} \begin{bmatrix} D & 0 & (-1)^kC_e & 0 \\ 0 & D & 0 & (-1)^kC_e \\ (-1)^kC_e & 0 & E & 0 \\ 0 & (-1)^kC_e & 0 & E \end{bmatrix}, \] (8)

where \( D = 2(1 - \kappa)N_y + 1 \), \( C_e = (2(1 - \kappa)\sqrt{\kappa}G^2 + 1 \), and \( E = 2(1 - \kappa)\sqrt{\kappa}G^2 + 2(1 - \kappa)N_y + 1 \). Eve too is interested in minimum error-probability decoding of Bob’s bit.

Alice’s minimum error-probability decision rule is to measure \( \hat{\rho}_{sl}^{(k)} - \hat{\rho}_{sr}^{(k)} \), 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 \( \hat{\rho}_{sr}^{(k)} - \hat{\rho}_{sr}^{(0)} \) 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

\[ \Pr(e) \leq e^{-M \max_{s=0,1} \{ \mathcal{E}(s) \}/2}, \] (9)

for

\[ \mathcal{E}(s) = -\ln(\text{tr}[\hat{\mu}_s^{(1)}(\hat{\mu}_s^{(1)})^{-1}]), \] (10)

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

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

The BPSK symmetry in \( \hat{\rho}_{sl}^{(k)} \) and \( \hat{\rho}_{sr}^{(k)} \) 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,

\[ \Pr(e) \geq \frac{1 - e^{-2M\mathcal{E}(1/2)}}{2}; \] (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 \( 4 \times 4 \) dimensional covariance matrix \( \Lambda \) consists of a \( 4 \times 4 \) dimensional symplectic matrix \( S \) and a symplectic spectrum \( \{ \nu_n; 1 \leq n \leq 2 \} \) that satisfy

\[ S \Omega S^T = \Omega = \begin{bmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & -1 & 0 \end{bmatrix}, \] (13)

\[ \Lambda = S \text{ diag}(\nu_1, \nu_1, \nu_2, \nu_2) S^T, \] (14)

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

For our quantum-illumination (Alice-to-Bob-to-Alice)
communication, the symplectic matrices needed for the diagonalization of $A^{(k)}_{B|I}$ are
\[
S^{(k)} = \begin{bmatrix}
X_+ & (-1)^k X_-
\end{bmatrix},
\]
for $k=0,1$. Here, $X_{\pm} = \text{diag}(x_{\pm}, x_{\pm})$ with
\[
x_{\pm} = \sqrt{\frac{A+S \pm \sqrt{(A+S)^2 - 4C_a^2}}{2(A+S)^2 - 4C_a^2}}.
\]
The associated symplectic spectra are identical for $k=0$ and 1, and $n=1,2$ we have
\[
\nu^{(k)}_n = \left[\left(-1\right)^n (S-A) + \sqrt{(A+S)^2 - 4C_a^2}\right]/8.
\]

For Eve’s attempt to listen in, the symplectic matrices needed for the diagonalization of $A^{(k)}_{S|R}$ are
\[
S^{(k)} = \begin{bmatrix}
Y & (-1)^k Z
\end{bmatrix},
\]
for $k=0,1$. Here, $Y = \text{diag}(\cos(\theta), \cos(\theta))$ and $Z = \text{diag}(\sin(\theta), \sin(\theta))$ with
\[
\cos(2\theta) = \frac{D-E}{\sqrt{(D-E)^2 + 4C_a^2}}.
\]
The associated symplectic spectra are identical for $k=0$ and 1, i.e., for $n=1,2$ we have
\[
\nu^{(k)}_n = \left[(D+E) - \left(-1\right)^n \sqrt{(D-E)^2 + 4C_a^2}\right]/8.
\]

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:
\[
\Pr(e)_{\text{Alice}} \leq \frac{\exp(-4M\kappa G N_S^2/N_B)}{2},
\]
\[
\Pr(e)_{\text{Eve}} \leq \frac{\exp(-4M(1-\kappa)G N_S^2/N_B)}{2},
\]
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
\[
\mathcal{E}_{\text{Alice}}(1/2)/\mathcal{E}_{\text{Eve}}(1/2) = 1/(1-\kappa)N_B \gg 1.
\]

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 accredit 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
\[
\hat{a}_m^\dagger = \sqrt{G_{\text{OPA}}} \hat{a}_m + \sqrt{G_{\text{OPA}} - 1} \hat{a}_m^\dagger,
\]
for $1 \leq m \leq M$,
\[
\text{where } G_{\text{OPA}} = 1 + N_S/\sqrt{\kappa N_B}. \text{ She then makes a minimum error-probability decision based on the results of the photon-counting measurement } \sum_m \hat{a}_m^\dagger \hat{a}_m [16]. \text{ The Bhattacharyya bound [17] on this receiver’s error probability in the } N_S \ll 1, \kappa N_B \gg 1 \text{ regime turns out to be}
\]
\[
\Pr(e)_{\text{OPA}} \leq \frac{\exp(-2M\kappa G N_S^2/N_B)}{2},
\]
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, Al-
ice must increase her mode-pair number $M$ at constant $N_L$ 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 $M=2 \times 10^5$, the case shown in Fig. 1 will yield 50 Mbit/s communication with

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

(26)

and

$$0.285 \leq \Pr(e)_{\text{Eve}} \leq 0.451$$

(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 $G_{\text{OPA}}=-1=0.00013$—the gain value needed for $N_L=0.004$, $\kappa =0.1$, and $N_0=10^3$—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 $\bar{N}_L=2.90 \times 10^5$ for $k=0$, and $2.33 \times 10^5$ 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, it is 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.

[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 $C_\gamma$ replaced by $C_\gamma=2 N_\gamma$. For low-brightness operation, wherein $N_L \ll 1$ prevails, we have $C_{\phi} \approx C_\gamma$.
[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 $\mu$m at 1.55 $\mu$m wavelength [N. S. Kopeika and J. Bordogna, Proc. IEEE 58, 1571 (1970)] leads to $\langle \hat{e}_B \hat{e}_B^\dagger \rangle \sim 10^{-6}$ for a line-of-sight terrestrial link; nighttime values are orders of magnitude lower. Room-temperature thermal noise is even weaker, viz., $\langle \hat{e}_B \hat{e}_B^\dagger \rangle = 4 \times 10^{-14}$ at 1.55 $\mu$m wavelength for a 300 K noise temperature. Thus, our pure-loss (noiseless) channel model will suffice so long as $N_\gamma \gg 10^{-6}$.
[11] For $N_\gamma \equiv \kappa G$, 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.

[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 \( \hat{E}(t) = \sum \hat{a}_m a_m e^{-i\omega_m t} / \sqrt{T} \) 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.