Near-field turbulence effects on quantum-key distribution

Jeffrey H. Shapiro
Massachusetts Institute of Technology, Research Laboratory of Electronics, Cambridge, Massachusetts 02139
(Received 27 September 2002; published 24 February 2003)

Bounds on average power transfer over a near-field optical path through atmospheric turbulence are used to deduce bounds on the sift and error probabilities of a free-space quantum-key distribution system that uses the Bennett-Brassard 1984 (BB84) protocol. It is shown that atmospheric turbulence imposes at most a modest decrease in the sift probability and a modest increase in the conditional probability of error given that a sift event has occurred.

DOI: 10.1103/PhysRevA.67.022309 PACS number(s): 03.67.Dd, 42.68.Bz, 42.50.Ar, 42.79.Sz

I. INTRODUCTION

Quantum-key distribution (QKD) has developed from the original proposal of Bennett and Brassard [1] into a technology that is on the verge of commercial viability. For most applications, the propagation medium of choice for QKD is low-loss optical fiber; see Ref. [2] for a number of experimental demonstrations of such fiber-based systems. On the other hand, there are a variety of QKD scenarios, such as communication involving mobile terminals, for which line-of-sight optical propagation through the atmosphere must be used. So-called free-space QKD systems, operating between terrestrial terminals separated by as much as 10 km, have been demonstrated [3], although the term free-space QKD is really a misnomer in this regard. In particular, there are nontrivial impairments—arising from molecular, aerosol, and turbulence effects—over atmospheric paths that would not be encountered were the propagation through vacuum, i.e., through free space. Nevertheless, in keeping with existing terminology we shall use free-space QKD to refer to systems operating over atmospheric paths, reserving the term vacuum propagation for cases in which there are no atmospherics whatsoever.

Previous work on free-space QKD has not adequately delineated the effects of atmospheric turbulence, viz., the random refractive-index variations that accompany turbulent mixing of air parcels with ~ 1 K temperature differences. Papers describing experimental systems comment on the impact of turbulence-induced scintillation [3], without quantifying its effects. A theoretical paper assessing the viability of free-space QKD [4] draws upon well-established statistical results for the phase and log-amplitude fluctuations produced by propagation through turbulence [5], but does not directly address the resulting QKD sift and error probabilities. Deriving upper and lower bounds on these probabilities is thus the main goal of the present paper. Although a great deal is known about optical communication error probabilities for the turbulent channel [6], these studies differ from the free-space QKD scenario in two respects. First, a conventional optical communication transmitter for the atmospheric channel produces sufficient photon flux to ensure an extremely low error probability (say between 10^{-9} and 10^{-6}), whereas a QKD transmitter constrains itself to a very low photon flux to preclude multiphoton security attacks and hence suffers an appreciable error probability ($\sim 10^{-2}$). Second, a conventional atmospheric optical communication system is typically configured for far-field operation, to minimize pointing or tracking requirements, whereas a free-space QKD system should operate in the near field, to maximize its key rate. It follows that our treatment of the sift and error probabilities for free-space QKD will differ, in significant respects, from prior work on optical communication through atmospheric turbulence. Indeed, the lognormal-fading analyses that dominate previous treatments of the turbulent atmospheric channel play no role in our near-field QKD study.

The remainder of this paper is organized as follows. In Sec. II we describe the BB84 QKD system whose sift and error probabilities are to be determined. In Sec. III we apply the normal-mode decomposition for propagation through turbulence [7] to obtain bounds on these probabilities. We conclude, in Sec. IV, with a numerical example and some discussion.

II. BB84 FREE SPACE QKD SYSTEM

The QKD system we consider uses a line-of-sight optical link to connect a transmitter (Alice, shown in Fig. 1) with a receiver (Bob, shown in Fig. 2). On each bit interval, Alice chooses randomly between two linear polarization bases, $0°/90°$ and $\mp 45°$, which we will denote $+$ and $\times$, respectively. Having chosen a basis, she sends a random bit value, 0 or 1, using the coding

$$0 \rightarrow \begin{cases} 0° & \text{if } + \text{ was chosen} \\ -45° & \text{if } \times \text{ was chosen,} \end{cases} \tag{1a}$$

$$1 \rightarrow \begin{cases} 90° & \text{if } + \text{ was chosen} \\ +45° & \text{if } \times \text{ was chosen.} \end{cases} \tag{1b}$$

Bob's receiver uses a passive 50/50 beam splitter to create inputs for a pair of polarization analysis systems—one for the $+$ basis and one for the $\times$ basis—that employ identical single-photon avalanche photodiodes (APDs), each of quantum efficiency η [11]. For a single photon arriving at Bob's receiver, this passive arrangement amounts to a random choice between the $+$ and the $\times$ measurement bases.

Let $\{N_{0°}, N_{90°}, N_{-45°}, N_{+45°}\}$ denote the photon counts from the four APDs during a single bit interval. Bob has a *detection* event when $N_{0°}+N_{90°}+N_{-45°}+N_{+45°}=1$, i.e., when exactly one of his detectors registers a count. In the

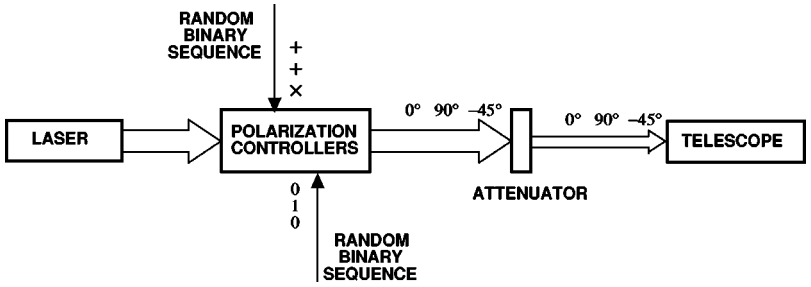

FIG. 1. Block diagram of a single-laser QKD transmitter (Alice). The laser output is a stream of linearly polarized pulses. The polarization controllers are driven by a pair of random binary sequences. The first sequence determines the sequence of polarization bases that will be sent: $+ = 0°/90°$ or $\times = \mp 45°$. The second sequence determines the bit value to be sent, according to the coding rule given in Eq. (1). The attenuator reduces the transmitter's output to n_S photons, on average, per bit interval.

BB84 protocol, Bob discloses to Alice the sequence of bit intervals and associated measurement bases for which he has detections. Alice then informs Bob which detections occurred in bases coincident with those that she used. These are the *sift* events, i.e., bit intervals in which Bob has a detection *and* his count has occurred in the same basis that Alice used. For example, if Alice sent her bit value as a 90°-polarized laser pulse, then a sift event means that Bob had detected exactly one count from his four detectors, with $N_{0°}=1$ or $N_{90°}=1$. An *error* event is a sift event in which Bob decodes the incorrect bit value. For example, if Alice sent her bit value as a 90°-polarized laser pulse, then an error event means that Bob had a sift in which $N_{0°}=1$ occurred. Once sift events have been identified, the remainder of the BB84 protocol—which shall not concern us in this paper—is standard. Alice and Bob follow a prescribed set of operations to identify errors in their sifted bits, correct these errors, and apply sufficient privacy amplification to deny useful key information to any potential eavesdropper (Eve). At the end of the full QKD procedure, Alice and Bob have a shared one-time pad with which they can communicate in complete security. For a given level of privacy amplification (security), the principal figure-of-merit for the BB84 QKD system is its key rate, i.e., the number of one-time pad bits/sec that Alice and Bob produce. Key rate decreases with decreasing sift probability and increasing error probability. Our objective is to determine the degree to which turbulence affects these probabilities [12].

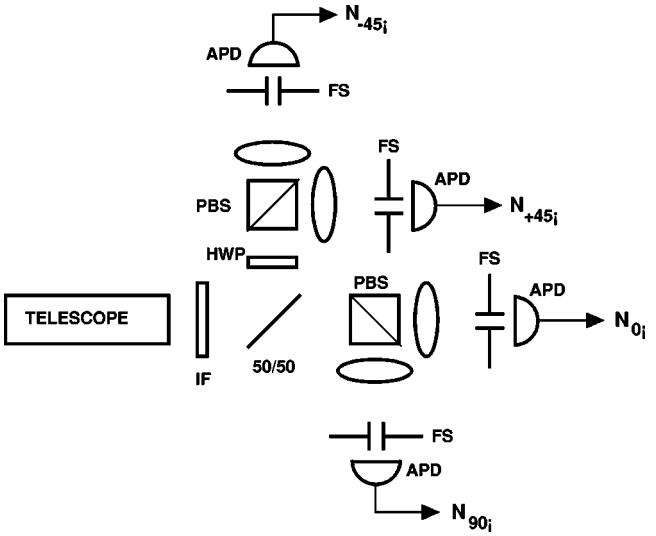

FIG. 2. Block diagram of a QKD receiver (Bob). IF, interference filter, provides spectral discrimination against background light. 50/50, ordinary beam splitter, provides a passive, random choice of polarization-analysis basis ($+$ or $\times$) for a single photon. HWP, half-wave plate, converts $\times$ basis into $+$ basis. PBS, polarizing beam splitter. FS, field stop, provides spatial-mode discrimination against background light. APD, single-photon (Geiger mode) avalanche photodiode.

We shall assume that Alice transmits an appropriately polarized laser signal pulse with an average photon number of n_S to represent her bit value. Bob's receiver will collect a random fraction γ of the transmitted photons owing to the combined effects of diffraction, atmospheric turbulence, and (absorption-plus-scattering induced) extinction [13]. In addition, Bob's receiver will collect n_B background photons per polarization, on average, and each of his detectors will be subject to a dark-current-equivalent average photon number of n_D. Let x,y be dummy variables each taking on the possible values $\{0°, 90°, -45°, +45°\}$. We then have the following statistics for the APD counts. Given that Alice sends an x-polarized signal and given the value of γ, the counts $\{N_{0°}, N_{90°}, N_{-45°}, N_{+45°}\}$ are statistically independent Poisson random variables [8] whose conditional means are [14],

$$E(N_y|x \text{ sent}, \gamma) = \begin{cases} \eta(n_S\gamma/2 + n_N) & \text{for } y = x \\ \eta n_N & \text{for } y \neq x, \text{ with } x,y \in + \\ \eta n_N & \text{for } y \neq x, \text{ with } x,y \in \times \\ \eta(n_S\gamma/4 + n_N) & \text{for } x \in + \text{ and } y \in \times \\ \eta(n_S\gamma/4 + n_N) & \text{for } x \in \times \text{ and } y \in +, \end{cases} \tag{2}$$

where $n_N \equiv n_B/2 + n_D$ is the average number of noise (background light plus dark-current-equivalent) photons reaching each detector. These conditional means presume perfect alignment between Alice's and Bob's polarization bases, and perfect polarization separation by the polarizing beam splitters in Bob's receiver.

It is now easy to find the sift and error probabilities conditioned on knowledge of γ:

$$\text{Prob}(\text{sift}|\gamma)=\eta(n_S\gamma/2+2n_N)e^{-\eta(n_S\gamma+4n_N)}, \tag{3}$$

$$\text{Prob}(\text{error}|\gamma)=\eta n_N e^{-\eta(n_S\gamma+4n_N)}. \tag{4}$$

To obtain the unconditional sift and error probabilities we need to average the preceding results using $p(\gamma)$, the probability density for the capture fraction γ:

$$\text{Prob}(\text{sift})=\int_0^1 d\gamma\, p(\gamma)\text{Prob}(\text{sift}|\gamma), \tag{5}$$

$$\text{Prob}(\text{error})=\int_0^1 d\gamma p(\gamma)\text{Prob}(\text{error}|\gamma). \tag{6}$$

III. NORMAL-MODE DECOMPOSITION AND PROBABILITY BOUNDS

The capture fraction γ is obtainable from the extended Huygens-Fresnel principle. Suppose that Alice transmits a normalized spatial beam pattern $\xi_0(\vec{\rho})$ from a diameter-d_1 circular exit pupil R_1 in the $z=0$ plane, and that Bob collects the light received from Alice within a diameter-d_2 entrance pupil R_2 in the $z=L$ plane that is coaxial with R_1. The field pattern $\xi_L(\vec{\rho}')$ generated in the $z=L$ plane from Alice's transmission of $\xi_0(\vec{\rho})$ satisfies [6],

$$\xi_L(\vec{\rho}')=\int_{R_1} d\vec{\rho}\,\xi_0(\vec{\rho})\frac{\exp(jkL+jk|\vec{\rho}-\vec{\rho}'|^2/2L)}{j\lambda L}$$
$$\times\exp[\chi(\vec{\rho}',\vec{\rho})+j\phi(\vec{\rho}',\vec{\rho})]\exp(-\alpha L/2). \tag{7}$$

In this equation, the fraction term within the integrand is the vacuum-propagation Green's function $h_L^o(\vec{\rho}'-\vec{\rho})$ for monochromatic (wavelength λ, wave number $k=2\pi/\lambda$), paraxial diffraction from $z=0$ to $z=L$. The χ and ϕ terms account for the stochastic log-amplitude and phase fluctuations, respectively, imposed by atmospheric turbulence. Thus,

$$h_L(\vec{\rho}',\vec{\rho})\equiv h_L^o(\vec{\rho}'-\vec{\rho})\exp[\chi(\vec{\rho}',\vec{\rho})+j\phi(\vec{\rho}',\vec{\rho})], \tag{8}$$

is the Green's function for $z=0$ to $z=L$ propagation through clear turbulent air, i.e., atmospheric propagation in the absence of extinction. The remaining exponential term in the Eq. (7) integrand accounts for extinction, viz., the loss that is due to absorption and scattering. Note that we have assumed this loss to be uniformly distributed along the $z=0$ to $z=L$ path with extinction coefficient α, although a nonuniform distribution is easily accommodated [15]. Within the weak-perturbation (Rytov) regime, $\chi(\vec{\rho}',\vec{\rho})$ and $\phi(\vec{\rho}',\vec{\rho})$ are jointly Gaussian random fields with known first and second moments [6].

With $\xi_0(\vec{\rho})$ normalized to satisfy

$$\int_{R_1} d\vec{\rho}\,|\xi_0(\vec{\rho})|^2=1, \tag{9}$$

the capture fraction γ is found from Eq. (7) via

$$\gamma=\int_{R_2} d\vec{\rho}'\,|\xi_L(\vec{\rho}')|^2. \tag{10}$$

Let us introduce the singular value (normal-mode) decomposition of Green's function $h_L(\vec{\rho}',\vec{\rho})$ [7],

$$h_L(\vec{\rho}',\vec{\rho})=\sum_{n=1}^{\infty}\sqrt{\mu_n}\phi_n(\vec{\rho}')\Phi_n^*(\vec{\rho})$$
$$\text{for } \vec{\rho}\in R_1 \text{ and } \vec{\rho}'\in R_2, \tag{11}$$

where $1\geq\mu_1\geq\mu_2\geq\mu_3\geq\cdots\geq 0$, and $\{\Phi_n(\vec{\rho})\}$ and $\{\phi_n(\vec{\rho}')\}$ are complete orthonormal (CON) function sets on R_1 and R_2, respectively. The eigenvalues $\{\mu_n\}$, the input eigenfunctions $\{\Phi_n(\vec{\rho})\}$ and the output eigenfunctions $\{\phi_n(\vec{\rho}')\}$ are, in general, random quantities, because we have made a singular value decomposition of a stochastic Green's function. For future use, we also introduce the corresponding decomposition of the vacuum-propagation Green's function, i.e.,

$$h_L^o(\vec{\rho}'-\vec{\rho})=\sum_{n=1}^{\infty}\sqrt{\mu_n^o}\phi_n^o(\vec{\rho}')\Phi_n^{o*}(\vec{\rho}),$$
$$\text{for } \vec{\rho}\in R_1 \text{ and } \vec{\rho}'\in R_2, \tag{12}$$

with $1\geq\mu_1^o\geq\mu_2^o\geq\mu_3^o\cdots\geq 0$, and $\{\Phi_n^o(\vec{\rho})\}$, $\{\phi_n^o(\vec{\rho}')\}$ CON on R_1 and R_2, respectively. Here, of course, the eigenvalues and eigenfunctions are deterministic, as there is no randomness in vacuum propagation.

In QKD we are interested in maximizing the capture fraction γ. From the singular value decomposition of $h_L(\vec{\rho}',\vec{\rho})$ we see that $\gamma\leq\mu_1 e^{-\alpha L}$ prevails, with equality when $\xi_0(\vec{\rho})=\Phi_1(\vec{\rho})$. In general, such an input distribution can only be achieved by adaptive optics techniques, although there are special cases for which $\Phi_1(\vec{\rho})$ is nonrandom. Because we are interested in the ultimate limits set by turbulence on the sift and error probabilities, we shall assume that Alice is able to employ the optimum field pattern in her transmitter, even if that calls for adaptive optics. To find the unconditional sift and error probabilities for this optimum transmitter, we now must find the statistics of μ_1, the maximum eigenvalue of the turbulent atmosphere's singular value decomposition. For near-field propagation, determining these statistics is a formidable task. Thus we shall content ourselves with easily derived bounds on $E(\mu_1)$, the average value of this eigenvalue. Results are available [9], however, for the free-space eigenvalue μ_1^o, which will allow us to compare our turbulence bounds on the sift and error probabilities with their nonturbulent (vacuum propagation attenuated by extinction) counterparts.

For both vacuum and turbulent propagation paths, we can distinguish the existence of far-field and near-field R_1-to-R_2 power transfer regimes according to whether their respective eigensums,

$$D_f^o \equiv \int_{R_1} d\vec{\rho} \int_{R_2} d\vec{\rho}\,' |h_L^o(\vec{\rho}\,' - \vec{\rho})|^2 = \sum_{n=1}^{\infty} \mu_n^o \tag{13}$$

and

$$D_f \equiv \int_{R_1} d\vec{\rho} \int_{R_2} d\vec{\rho}\,' |h_L(\vec{\rho}\,', \vec{\rho})|^2 = \sum_{n=1}^{\infty} \mu_n, \tag{14}$$

are much less than (far field) or much greater than (near field) unity [7]. In the far field, $\mu_1^o \approx D_f^o \ll 1$ and $\mu_1 \approx D_f \ll 1$ prevail, indicating, in each case, that there is only a single input mode that couples appreciable power from R_1 to R_2. In the near field, there are $\approx D_f^o$ near-unity vacuum-propagation eigenvalues and $\approx D_f$ near-unity turbulent-propagation eigenvalues, corresponding, in each case, to the number of pixels that the R_2 pupil could resolve within R_1 [16]. From Eqs. (7) and (13) we have that D_f^o equals the Fresnel number product of the R_1 and R_2 pupils,

$$D_f^o = \left(\frac{\pi d_1 d_2}{4\lambda L} \right)^2, \tag{15}$$

and the statistics of the log-amplitude fluctuation $\chi(\vec{\rho}\,', \vec{\rho})$ imply that $E(D_f) = D_f^o$ [7]. This last result yields the upper bound

$$E(\mu_1) \leqslant \mu_{\rm UB} \equiv \min(1, D_f^o), \tag{16}$$

we shall also need a lower bound on $E(\mu_1)$. Because $E(\mu_1)$ is the maximum average power transfer achievable over the turbulent R_1-to-R_2 path, it is lower bounded by the average power transfer of any normalized input function $\xi_0(\vec{\rho})$. As discussed in Ref. [7], the normalized focused beam,

$$\xi_0(\vec{\rho}) = \sqrt{\frac{4}{\pi d_1^2}} \exp(-jk|\vec{\rho}|^2/2L) \quad \text{for } \vec{\rho} \in R_1, \tag{17}$$

is a good choice in this regard, leading to the lower bound

$$E(\mu_1) \geqslant \mu_{\rm LB} \equiv \int_0^1 dx (8\sqrt{D_f^o}/\pi) \exp[-D(d_1 x)/2] \times (\cos^{-1}(x) - x\sqrt{1-x^2}) J_1(4x\sqrt{D_f^o}), \tag{18}$$

where

$$D(\rho) = 1.09 k^2 C_n^2 L \rho^{5/3} \tag{19}$$

is the spherical-wave wave structure function with C_n^2 being the turbulence-strength constant along the propagation path [17], and $J_1(\cdot)$ being the first-order Bessel function of the first kind.

It is now a simple matter to obtain the desired results for the unconditional sift and error probabilities. We shall assume that Alice employs the optimum normalized spatial beam pattern at her transmitter: $\xi_0(\vec{\rho}) = \Phi_1^o(\vec{\rho})$ for the case of nonturbulent propagation, and $\xi_0(\vec{\rho}) = \Phi_1(\vec{\rho})$ for the case of atmospheric propagation, recognizing that the latter may require the use of adaptive optics. Vacuum propagation suffers no fading, whence

$$\text{Prob(sift)} = (\eta/2)(n_S \mu_1^o e^{-\alpha L} + 4n_N) e^{-\eta(n_S \mu_1^o e^{-\alpha L} + 4n_N)}, \tag{20}$$

$$\text{Prob(error)} = \eta n_N e^{-\eta(n_S \mu_1^o e^{-\alpha L} + 4n_N)}, \tag{21}$$

for nonturbulent propagation. Moreover, because $f(x) \equiv x e^{-x}$ is a convex function for $0 \leqslant x < 2$ whose derivative is positive for $0 \leqslant x < 1$, it follows that,

$$\text{Prob(sift)} \leqslant (\eta/2)[n_S \mu_{\rm UB} e^{-\alpha L} + 4n_N] e^{-\eta(n_S \mu_{\rm UB} e^{-\alpha L} + 4n_N)} \tag{22}$$

and

$$\text{Prob(sift)} \geqslant \eta 2 n_N e^{-\eta 4 n_N}[1 - \mu_{\rm LB}] + (\eta/2)(n_S e^{-\alpha L} + 4n_N) \times e^{-\eta(n_S e^{-\alpha L} + 4n_N)} \mu_{\rm LB}, \tag{23}$$

for atmospheric propagation, under the condition that $\eta(n_S e^{-\alpha L} + 4n_N) < 1$. Likewise, because $g(x) = e^{-x}$ is a concave function with a negative derivative for $x \geqslant 0$, we can show that

$$\text{Prob(error)} \geqslant \eta n_N e^{-\eta[n_S \mu_{\rm UB} e^{-\alpha L} + 4n_N]} \tag{24}$$

and

$$\text{Prob(error)} \leqslant \eta n_N e^{-\eta 4 n_N}[1 - \mu_{\rm LB}] + \eta n_N e^{-\eta(n_S e^{-\alpha L} + 4n_N)} \mu_{\rm LB}. \tag{25}$$

Although these bounds apply in both the far field and the near field, our primary interest is in the near-field regime, wherein $D_f^o \geqslant 1$.

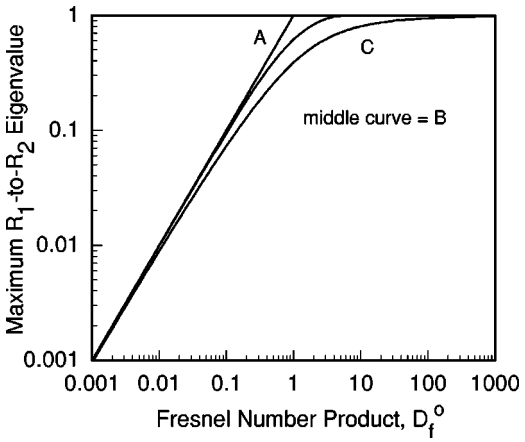

FIG. 3. Upper bound on average of maximum turbulence eigenvalue $\mu_{\rm UB}$ (curve *A*), vacuum-propagation maximum eigenvalue (curve *B*), and lower bound on average of maximum turbulence eigenvalue $\mu_{\rm LB}$ (curve *C*), versus Fresnel number product D_f^o. The $\mu_{\rm LB}$ plot assumes $d_1 = d_2$ operation in a $\sigma_\chi^2 = 0.1$ scintillation propagation environment.

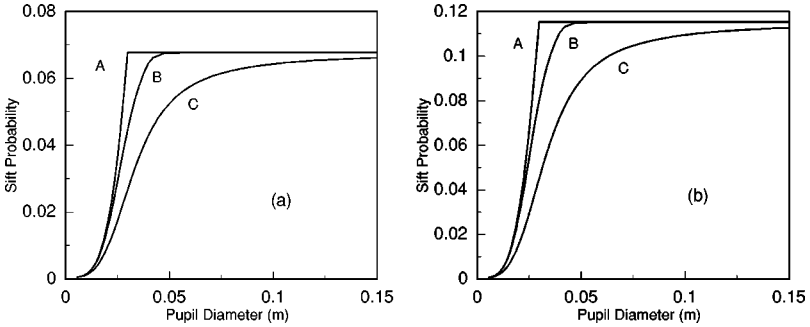

FIG. 4. Sift probability versus pupil diameter for equal aperture diameters, $d_1=d_2$: (a) $n_S=0.5$, (b) $n_S=1.0$. In both (a) and (b) curve *A* is the sift-probability upper bound for the turbulent channel, curve *B* is the sift probability for the nonturbulent case, and curve *C* is the sift-probability lower bound for the turbulent channel. The turbulent cases assume operation in a $\sigma_\chi^2=0.1$ propagation environment.

IV. EXAMPLE AND DISCUSSION

In this section we shall instantiate the bounds Eqs. (22)–(25), and compare them with the exact results for nonturbulent propagation, namely, Eqs. (20) and (21). In all that follows we shall assume operation at $\lambda=0.7$ μm wavelength, with $\alpha=2$ dB/km, $L=1$ km, $\eta=0.5$, $n_B=10^{-3}$, and $n_D=10^{-6}$. The η and n_D values are consistent with available silicon Geiger-mode APD technology at this wavelength, with a $T=1$ ns transmitter pulse duration. The n_B value is in the range of typical daytime operation at this wavelength using a receiver field of view that is ten times the diffraction limit. The 2 dB/km extinction coefficient corresponds to reasonably clear weather—visibility roughly 10 km. For the turbulence cases, we shall employ a uniform $C_n^2=2\times10^{-14}$ m$^{-2/3}$ turbulence distribution along the propagation path, representing moderate turbulence for a near-ground path.

We begin our calculations by examining the behavior of eigenvalue bounds, $\mu_{\rm LB}$ and $\mu_{\rm UB}$, as compared to the vacuum-propagation eigenvalue, μ_1^o. Figure 3 plots all three of these quantities versus the Fresnel number product D_f^o under the assumption that the $d_1=d_2$, i.e., that the transmit and receive apertures have equal diameters. Interestingly, whereas $\mu_{\rm UB}$ only depends on D_f^o, and the same is known to be true [9] for μ_1^o, the equal-diameter case provides a worst-case lower bound on $E(\mu_1)$ for a given value of D_f^o [7]. This is because $\mu_{\rm LB}$ is an increasing function of decreasing d_1 at constant D_f^o *and* atmospheric reciprocity [10] can be used to show that

$$E(\mu_1)\geqslant\mu'_{\rm LB}\equiv\int_0^1 dx(8\sqrt{D_f^o/\pi})\exp[-D(d_2x)/2]\times[\cos^{-1}(x)-x\sqrt{1-x^2}]J_1(4x\sqrt{D_f^o}). \quad (26)$$

So, because the symmetric ($d_1=d_2$) case may be the most convenient in practice, we shall limit our consideration to this worst-case scenario. It is then worth noting that

$$D(\rho)=51.0\sigma_\chi^2(D_f^o)^{5/12}\rho^{5/3} \quad (27)$$

when $d_1=d_2$, where

$$\sigma_\chi^2=0.124C_n^2k^{7/6}L^{11/6} \quad (28)$$

is the spherical-wave log-amplitude variance, viz., the scintillation strength. For our assumed parameter values, $\sigma_\chi^2=0.1$ prevails.

Figure 3 clearly exhibits near-field characteristics, $\mu_1^o\to1$ and $1\geqslant E(\mu_1)\geqslant\mu_{\rm LB}\to1$ as $D_f^o\to\infty$. Applying these eigenvalue results to the QKD sift and error probabilities we obtain the plots shown in Figs. 4 and 5, respectively. These figures demonstrate that $\sigma_\chi^2=0.1$ scintillation has a very modest effect on the sift and error probabilities in worst-case (equal aperture) near-field operation. In particular, suppose that $d_1=d_2=5.31$ cm, so that $D_f^o=10$ for $\lambda=0.7$ μm and $L=1$ km. Here we find that the nonturbulent Prob(sift) $=0.068$ as compared to the turbulence lower bound of 0.054 when $n_s=0.5$, and Pr(sift)$=0.115$ for the nonturbulent case versus a turbulence lower bound of 0.093 when $n_S=1.0$. In

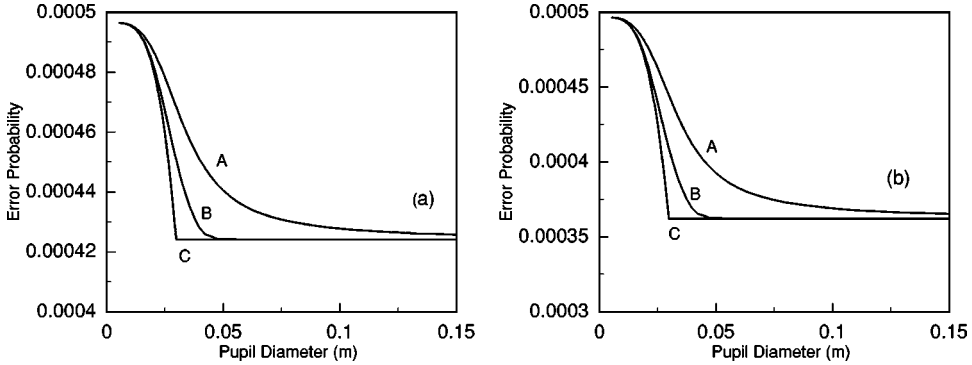

FIG. 5. Error probability versus pupil diameter for equal aperture diameters, $d_1=d_2$: (a) $n_S=0.5$, (b) $n_S=1.0$. In both (a) and (b) curve *A* is the error-probability upper bound for the turbulent channel, curve *B* is the error probability for the nonturbulent case, and curve *C* is the error-probability lower bound for the turbulent channel. The turbulent cases assume operation in a $\sigma_\chi^2=0.1$ propagation environment.

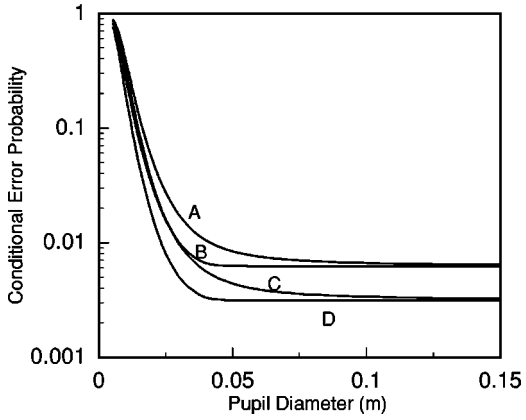

FIG. 6. Conditional probability of error, given that a sift event has occurred, versus pupil diameter for equal aperture diameters, $d_1=d_2$. Curve A, upper bound on Pr(error|sift) for the turbulent channel when $n_S=0.5$; curve B, nonturbulent Pr(error|sift) when $n_S=0.5$; curve C, upper bound on Pr(error|sift) for the turbulent channel when $n_S=1.0$; and curve D nonturbulent Pr(error|sift) when $n_S=1.0$. The turbulent cases assume operation in a $\sigma_\chi^2=0.1$ propagation environment.

other words, at $D_f^o=10$, the near-field sift probability in the presence of turbulence is *at least* 80% of its value in the absence of turbulence. Although similar comments can be made, from Fig. 5, comparing the near-field error probabilities in the absence and presence of turbulence, it is more interesting to consider the conditional probability of error, given that a sift event has occurred,

$$\text{Prob}(\text{error}|\text{sift}) \equiv \frac{\text{Prob}(\text{error})}{\text{Prob}(\text{sift})}, \tag{29}$$

because it is this conditional probability that directly measures the amount of error correction which must be employed in the BB84 protocol. Figure 6 compares the nonturbulent results for Prob(error|sift) with the turbulence upper bound, where the latter is obtained by employing Eqs. (25) and (23), respectively, in the numerator and denominator of Eq. (29). Here we find, for $d_1=d_2=5.31$ cm (corresponding to $D_f^o=10$), that nonturbulent Prob(error|sift)$=6.28\times10^{-3}$ when $n_S=0.5$, and it equals 3.15×10^{-3} when $n_S=1.0$. The corresponding turbulence upper bounds are 8.06×10^{-3} and 4.20×10^{-3}. Thus, the presence of turbulence causes *at most* 28% and 39% increases in conditional error probability at these n_S values.

Some final comments are now in order. We have used near-field power transfer analysis to obtain bounds on the sift and error probabilities of a free-space BB84 QKD system. These bounds show that turbulence effects will be quite modest in the near-field regime. In this regard, it is important to note how conservative our results are. First of all, Eqs. (23) and (25)—which determine our upper bound on the conditional probability of error given that a sift event has occurred—are obtained by assigning the worst-case probability density,

$$p(\zeta)=[1-\mu_{\text{LB}}]\delta(\zeta)+\mu_{\text{LB}}\delta(\zeta-1), \tag{30}$$

where $\delta(\cdot)$ is the unit impulse (Dirac δ) function, to the focused-beam power transfer through the turbulence, viz.,

$$\zeta \equiv \int_{R_2} d\vec{\rho}\,' \left| \int_{R_1} d\vec{\rho}\, \sqrt{\frac{4}{\pi d_1^2}} e^{-jk|\vec{\rho}|^2/2L} h_L(\vec{\rho}\,',\vec{\rho}) \right|^2 . \tag{31}$$

The actual $p(\zeta)$ will not be concentrated at $\zeta=0,1$, hence it will have a lower variance than that of Eq. (30), leading to a higher value for the sift probability and a lower value for the error probability for the same value of $\mu_{\text{LB}}=E(\zeta)$. Moreover, although we indicated that adaptive optics will, in general, be required to achieve optimum R_1-to-R_2 power transfer over a turbulent path, our bounds do *not* use adaptive optics. In particular, the performance results we have presented apply to a nonadaptive system that employs the focused beam pattern given in Eq. (17). Thus, with the use of adaptive optics a higher average capture fraction than $\mu_{\text{LB}}e^{-\alpha L}$ should be achievable, bringing the performance in turbulence even closer to that of the nonturbulent case [18]. Finally, we must recognize that the near-field regime will not encompass all likely free-space QKD applications. If we take $D_f^o=10$ at $\lambda=0.7$ μm as our target near-field configuration, then path lengths as long as $L=20$ km can be reached with $d_1=d_2\leqslant 24$ cm. We should note, however, that focused beams of this diameter and wavelength require pointing to microradian accuracy for our analysis to apply. Thus, platform vibrations and mobile-terminal dynamics would mandate the use of closed-loop pointing and tracking. At even longer path lengths—such as those needed for QKD between a satellite and a ground terminal—the near-field ceases to be an accessible operating regime. A QKD sift and error probability analysis for far-field operation through atmospheric turbulence can be developed, from the extended Huygens-Fresnel principle, but this will be the subject of another paper.

ACKNOWLEDGMENT

This work was sponsored by the Department of the Air Force under Air Force Contract No. F19628-00-C-0002. Opinions, interpretations, conclusions, and recommendations are those of the author and are not necessarily endorsed by the United States Air Force.

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

[2] J.D. Franson and H. Ilves, Appl. Opt. **33**, 2949 (1994); C. Marand and P.D. Townsend, Opt. Lett. **20**, 1695 (1995); A. Muller, H. Zbinden, and N. Gisin, Europhys. Lett. **33**, 335 (1996); R.J. Hughes, G.L. Morgan, and C.G. Peterson, J. Mod.

Opt. **47**, 533 (2000); P.A. Hiskett, G. Bonfrate, G.S. Buller, and P.D. Townsend, *ibid.* **48**, 1957 (2001); D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, New J. Phys. **4**, 41 (2002).

[3] B.C. Jacobs and J.D. Franson, Opt. Lett. **21**, 1854 (1996); W.T. Buttler, R.J. Hughes, S.K. Lamoreaux, G.L. Morgan, J.E. Nordholt, and C.G. Peterson, Phys. Rev. Lett. **84**, 5652 (2000); J.G. Rarity, P.R. Tapster, and P.M. Gorman, J. Mod. Opt. **48**, 1887 (2001); R.J. Hughes, J.E. Nordholt, D. Derkacs, and C.G. Peterson, New J. Phys. **4**, 43 (2002).

[4] G. Gilbert and M. Hamrick, e-print quant-ph/0009027.

[5] V. I. Tatarksii, *The Effects of the Turbulent Atmosphere on Wave Propagation*, Israel Program for Scientific Translations (Israel Program for Scientific Translations, Jerusalem, 1971); *Laser Beam Propagation in the Atmosphere*, edited by J. W. Strohbehn (Springer-Verlag, Berlin, 1978); A. Ishimaru, *Wave Propagation and Scattering in Random Media* (Academic, New York, 1978); L. C. Andrews and R. L. Phillips, *Laser Beam Propagation through Random Media* (SPIE, Bellingham, 1998).

[6] J. H. Shapiro, in *Laser Beam Propagation in the Atmosphere*, edited by J. W. Strohbehn (Springer-Verlag, Berlin, 1978); J.H. Shapiro and R.C. Harney, Proc. SPIE **295**, 41 (1981).

[7] J.H. Shapiro, Appl. Opt. **13**, 2614 (1974).

[8] R. M. Gagliardi and S. Karp, *Optical Communications* (Wiley, New York, 1976).

[9] D. Slepian, J. Opt. Soc. Am. **55**, 1110 (1965).

[10] J.H. Shapiro, J. Opt. Soc. Am. **61**, 492 (1971).

[11] We will neglect optics losses within Bob's receiver; they can be accounted for by regarding η as the overall detection efficiency, i.e., the product of optics transmission and detector quantum efficiency.

[12] We could also address the detection probability, but, because Bob's receiver makes a random polarization-basis choice on each photon it measures, the detection probability is exactly twice the sift probability.

[13] Because Bob's receiver will employ a narrow field of view—to minimize background light shot noise—it will collect only the turbulence-modified extinguished direct beam from Alice's transmitter, i.e., no scattered light will be collected. Moreover, for bit durations that are appreciably shorter than 1 ms and appreciably longer than 1 ps, we can neglect time-dependent fading and multipath spread, and, because atmospheric turbulence is nondepolarizing, we then have that attenuation by the capture fraction γ is the only propagation effect incurred by Alice's transmitted pulse en route to Bob's receiver.

[14] By assuming conditionally-Poisson statistics we are ignoring the dead-time and after-pulsing limitations that are encountered with Geiger-mode APDs. These effects set a minimum value for the bit-interval duration, and preclude detection of more than one photon during such an interval. Conditionally-Poisson statistics can be used to analyze such a detector by replacing N_x with N_x' in our definitions of the detection, sift and error events, where $N_x'=0$ if $N_x=0$, and $N_x'=1$ if $N_x \geqslant 1$, for $x \in \{0°, 90°, -45°, 45°\}$. We shall employ the conditionally-Poisson statistics *without* such a replacement, i.e., we are assuming a multiphoton detection capability at each detection port in Fig. 2.

[15] A nonuniform distribution of extinction loss would mean $\exp(-\alpha L/2)$ should be replaced with $\exp[-\int_0^L dz \alpha(z)/2]$ in Eq. (7), where $\alpha(z)$ is the z-dependent extinction coefficient along the path from the transmitter to the receiver.

[16] Adaptive optics would, in general, be required for the turbulent case to achieve this resolution.

[17] For simplicity, we have assumed a uniform turbulence distribution from $z=0$ to $z=L$. For a nonuniform distribution, $1.09 C_n^2 L$ in Eq. (19) should be replaced with $2.91 \int_0^L dz C_n^2(z) \times (1-z/L)^{5/3}$.

[18] It is worth mentioning that an adaptive optics QKD implementation will require pilot-beam transmission to provide a strong signal for atmospheric wave-front sensing.