Scintillation has minimal impact on far-field Bennett-Brassard 1984 protocol quantum key distribution

Scintillation has minimal impact on far-field Bennett-Brassard 1984 protocol quantum key distribution

Jeffrey H. Shapiro
Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA
(Received 17 December 2010; published 27 September 2011)

The effect of scintillation, arising from propagation through atmospheric turbulence, on the sift and error probabilities of a quantum key distribution (QKD) system that uses the weak-laser-pulse version of the Bennett-Brassard 1984 (BB84) protocol is evaluated. Two earth-space scenarios are examined: satellite-to-ground and ground-to-satellite transmission. Both lie in the far-field power-transfer regime. This work complements previous analysis of turbulence effects in near-field terrestrial BB84 QKD [J. H. Shapiro, Phys. Rev. A **67**, 022309 (2003)]. More importantly, it shows that scintillation has virtually no impact on the sift and error probabilities in earth-space BB84 QKD, something that has been implicitly assumed in prior analyses for that application. This result contrasts rather sharply with what is known for high-speed laser communications over such paths, in which deep, long-lived scintillation fades present a major challenge to high-reliability operation.

DOI: 10.1103/PhysRevA.84.032340 PACS number(s): 03.67.Dd, 42.68.Bz, 42.50.Ar, 42.79.Sz

I. INTRODUCTION

In [1] we used the normal-mode decomposition for line-of-sight optical propagation through atmospheric turbulence [2] to obtain upper and lower bounds on the sift and error probabilities of a free-space optical implementation [3] of the Bennett-Brassard 1984 (BB84) protocol for quantum key distribution (QKD). There we focused on modest-length terrestrial paths, for which the transmit and receive pupils could easily be large enough that operation is in the near-field power-transfer regime. Earth-space BB84 QKD is being considered for transcontinental to worldwide applications, and these configurations are in the far-field power-transfer regime. To date, almost all assessments of the impact of atmospheric propagation on such far-field systems have not included scintillation [4]; i.e., only the effects of atmospheric extinction, turbulence-induced beam spread and angular spread, and background-light collection have been quantified (see, e.g., [5]). In this paper we rectify that deficiency. In particular, we show that scintillation has virtually no effect on the sift and error probabilities of a BB84 QKD system that uses satellite-to-ground or ground-to-satellite transmission. This result contrasts rather sharply with what is known for high-speed laser communications over such paths, in which deep and long-lived scintillation fades present a major challenge—arguably *the* major challenge—to high-reliability operation.

The rest of this paper is organized as follows. In Sec. II we briefly describe the BB84 QKD protocol that is treated and give expressions for its sift and error probabilities conditioned on knowledge of the fractional transmitter-to-receiver power transfer. These conditional probabilities are independent of whether operation is in the near-field or far-field power-transfer regimes, so they are available from [1] for the weak-laser-pulse system that we consider. In Sec. III we address the satellite-to-ground link. Using a lognormal-fading model we show that aperture-averaged scintillation has a negligible effect on the unconditional sift and error probabilities [6]. Section IV presents a similar analysis for two versions of the ground-to-satellite link. The first employs a collimated-beam (nonadaptive) transmitter. The second is an ideal adaptive-optics transmitter that perfectly tracks the maximum power-transfer input eigenfunction for the ground-to-space path. In both cases the conclusion reached is the same as that found in the satellite-to-ground analysis, viz., scintillation has a negligible effect on the unconditional sift and error probabilities.

II. SIFT AND ERROR PROBABILITIES FOR BB84 FREE-SPACE QKD

The QKD system we consider is the one described in [1]. It 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° or 90° and $\mp 45^\circ$, which we denote $+$ and $\times$, respectively. Having chosen a basis, she sends a random bit value, 0 or 1, using the coding

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

$$1 \longrightarrow \begin{cases} 90^\circ, & \text{if } + \text{ was chosen,} \\ +45^\circ, & \text{if } \times \text{ was chosen.} \end{cases} \tag{1b}$$

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

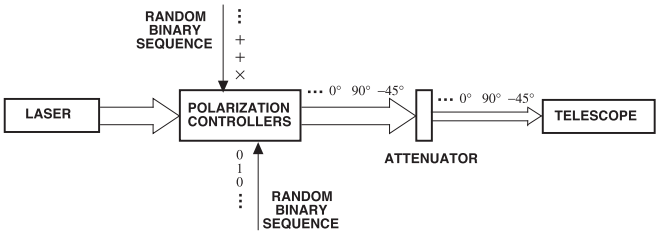

FIG. 1. Block diagram of a single-laser QKD transmitter (Alice). The laser output is a stream of linearly polarized pulses. The polarization controllers are driven by a pair of random binary sequences. The first sequence determines the sequence of polarization bases that will be sent: $+ = 0^\circ$ or 90° and $\times = \mp 45^\circ$. 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.

$N_{90^\circ} = 1$. 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 $N_{0^\circ} = 1$ occurred. Once sift events have been identified, the remainder of the BB84 protocol—which does 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 secrecy. For a given level of privacy amplification (secrecy), the principal figure of merit for the BB84 QKD system is its key rate, i.e., the number of one-time pad bits per second that Alice and Bob produce.

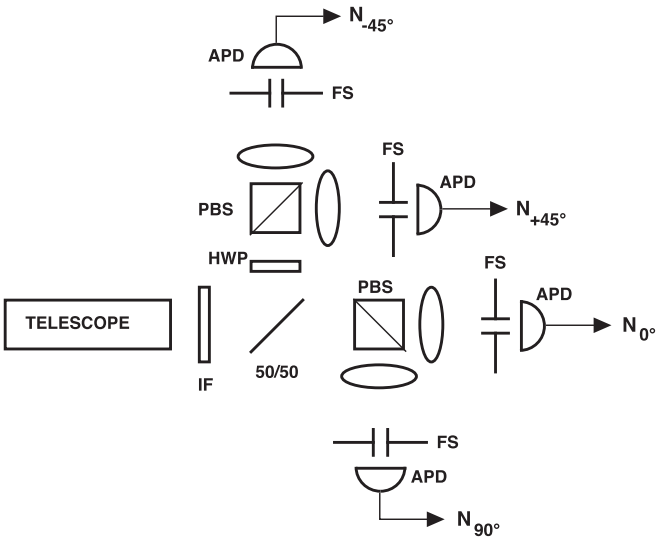

FIG. 2. Block diagram of a QKD receiver (Bob): IF, interference filter, provides spectral discrimination against background light; 50:50, ordinary beam splitter, provides a passive, random choice of polarization-analysis basis ($+$ or $\times$) for a single photon; HWP, half-wave plate, converts $\times$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

The key rate decreases with decreasing sift probability and increasing error probability. Our objective is to determine the degree to which turbulence affects these probabilities [8].

As in [1], we 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 collects a random fraction, γ, of the transmitted photons owing to the combined effects of diffraction, atmospheric turbulence, and (absorption-plus-scattering-induced) extinction. Indeed, because Bob's receiver employs a narrow field of view—to minimize background-light shot noise—it collects only the turbulence-modified extinguished direct beam from Alice's transmitter; i.e., no scattered light is 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. In addition, Bob's receiver collects n_B background photons per polarization, on average, and each of his detectors is subject to a dark-current-equivalent average photon number of n_D.

Again following [1], we assume our detectors have photon-number resolution capability and that the their dead time and afterpulsing can be neglected, so that they are governed by conditionally Poisson counting statistics. We then have that the conditional sift and error probabilities, given the fractional power transfer γ [9], are

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

and

$$\text{Prob(error} \mid \gamma) = \eta n_N e^{-\eta(n_S\gamma+4n_N)}, \tag{3}$$

where $n_N \equiv n_B/2 + n_D$ is the average number of noise (background light plus dark-equivalent) photons reaching each detector. Taking $0 < \mathcal{L} < 1$ to be the atmospheric extinction encountered along the propagation path, we write $\gamma = \mu\mathcal{L}$, where μ differs from its diffraction-limited (vacuum propagation) value solely because of atmospheric turbulence.

Our interest is in the *unconditional* sift and error probabilities, i.e.,

$$\text{Prob(sift)} = \int_0^1 d\mu\; p(\mu)\eta(n_S\mu\mathcal{L}/2 + 2n_N)e^{-\eta(n_S\mu\mathcal{L}+4n_N)} \tag{4}$$

and

$$\text{Prob(error)} = \int_0^1 d\mu\; p(\mu)\eta n_N e^{-\eta(n_S\mu\mathcal{L}+4n_N)}, \tag{5}$$

where $p(\mu)$ is the probability density function (PDF) for the random variable μ.

Consider far-field propagation from the ground ($z = 0$) to a satellite ($z = L$), or vice versa, in the absence of turbulence. In either case a collimated-beam transmitter realizes a deterministic fractional power transfer given by [10]

$$\gamma_{\text{NT}} = \mu_{\text{NT}}\mathcal{L} = \left(\frac{\pi D_G D_S}{4\lambda L}\right)^2 \mathcal{L} \ll 1, \tag{6}$$

where D_G and D_S are the diameters of the circular exit-entrance ground and satellite pupils, λ is the laser wavelength,

L is the path length,

$$\mathcal{L} = \exp\left(-\int_0^L dz\,\alpha(z)\right) \tag{7}$$

gives the extinction along the path in terms of the local extinction coefficient, $\alpha(z)$, and the subscript NT denotes "no turbulence." In this case we have $p(\mu) = \delta(\mu - \mu_{\rm NT})$, where $\delta(\cdot)$ is the impulse function, so that

$$\text{Prob(sift)}_{\rm NT} = \eta(n_S\mu_{\rm NT}\mathcal{L}/2 + 2n_N)e^{-\eta(n_S\mu_{\rm NT}\mathcal{L}+4n_N)} \tag{8}$$

and

$$\text{Prob(error)}_{\rm NT} = \eta n_N e^{-\eta(n_S\mu_{\rm NT}\mathcal{L}+4n_N)} \tag{9}$$

are the no-turbulence sift and error probabilities.

To proceed further we consider satellite-to-ground and ground-to-satellite scenarios, so that we can employ specific PDFs for μ and evaluate Prob(sift) and Prob(error).

III. SATELLITE-TO-GROUND SCENARIO

Consider the satellite-to-ground scenario in which the satellite's diameter-D_S exit pupil lies well within a single turbulence coherence area but the ground terminal's diameter-D_G entrance pupil comprises many turbulence coherence areas. In this case the extended Huygens-Fresnel principle leads to the following expression for the no-extinction fractional power transfer, assuming that the ground detector's field of view is large enough to capture all the laser light reaching the ground terminal's entrance pupil [11]:

$$\mu = \frac{\pi D_S^2}{4(\lambda L)^2}\int_{|\boldsymbol{\rho}|\leqslant D_G/2} d\boldsymbol{\rho}\, e^{2\chi(\mathbf{0},\boldsymbol{\rho})}. \tag{10}$$

Here, $\chi(\mathbf{0},\boldsymbol{\rho})$ is the log-amplitude fluctuation imposed on the field received at transverse coordinate $\boldsymbol{\rho}$ in the $z = 0$ plane from a point source radiating from transverse coordinate $\mathbf{0}$ in the $z = L$ plane. Energy conservation implies that

$$\langle e^{2\chi(\mathbf{0},\boldsymbol{\rho})}\rangle = 1, \tag{11}$$

where $\langle\cdot\rangle$ denotes ensemble average, from which

$$\langle\mu\rangle = \left(\frac{\pi D_G D_S}{4\lambda L}\right)^2 = \mu_{\rm NT}. \tag{12}$$

Equation (12) represents well-known downlink behavior; i.e., there is no beam spread due to turbulence when the transmitter pupil lies within a single coherence area, so the average power transfer is unaffected by turbulence if the receiver's field of view is sufficient to accommodate any turbulence-induced angular spread [12].

At this point, we assume that $\chi(\mathbf{0},\boldsymbol{\rho})$ is Gaussian distributed, statistically homogeneous, and isotropic. Thus it is completely characterized by its mean m_χ, variance σ_χ^2, and covariance function

$$K_{\chi\chi}(\rho) \equiv \langle\Delta\chi(\mathbf{0},\boldsymbol{\rho})\Delta\chi(\mathbf{0},\mathbf{0})\rangle, \tag{13}$$

with $\rho = |\boldsymbol{\rho}|$ and $\Delta\chi(\mathbf{0},\boldsymbol{\rho}) \equiv \chi(\mathbf{0},\boldsymbol{\rho}) - m_\chi$. The energy conservation condition in Eq. (12) then implies that $m_\chi = -\sigma_\chi^2$. Furthermore, because the sum of real-valued lognormal random variables is well approximated by a real-valued lognormal random variable [13], we can write [14]

$$\mu = \mu_{\rm NT}e^{2u}, \tag{14}$$

where u is a Gaussian random variable with mean $-\sigma_u^2$ and variance σ_u^2, with

$$e^{4\sigma_u^2} - 1 = \frac{4}{\pi D_G^2}\int_0^{D_G} d\rho\,\rho(e^{4K_{\chi\chi}(\rho)} - 1) \times\frac{2}{\pi}\left[\cos^{-1}(\rho/D_G) - (\rho/D_G)\sqrt{1-(\rho/D_G)^2}\right]. \tag{15}$$

Equation (15) is an aperture-averaging formula; viz., it amounts to

$$e^{4\sigma_u^2} - 1 = \frac{e^{4\sigma_\chi^2} - 1}{N_\chi(D_G)}, \tag{16}$$

where $N_\chi(D_G) \gg 1$ by assumption is the number of log-amplitude coherence areas in the ground terminal's entrance pupil.

Unfortunately, the lognormal distribution for μ does not permit us to obtain closed-form expressions for the sift and error probabilities. So, to demonstrate that scintillation has essentially no effect on these probabilities, we take a numerical approach, employing a worst-case value for σ_u^2. In particular, we choose $\sigma_\chi^2 = 0.5$, which is a conservative upper bound on saturated scintillation, and use $N_\chi(D_G) = 1$ in Eq. (16), thus obtaining a worst-case value $\sigma_u^2 = 0.5$. Using the reasonable values $n_S = 0.5$, $n_N = 5\times10^{-6}$, $\eta = 0.5$, and $\gamma_{\rm NT} = 10^{-3}$, we find

$$\text{Prob(sift)}_{\rm NT} = 1.299\times10^{-4} \tag{17}$$

and

$$\text{Prob(error)}_{\rm NT} = 2.499\times10^{-6}. \tag{18}$$

Using a lognormal distribution for u with $m_u = -\sigma_u^2 = -0.5$ we then find that

$$\left|\frac{\text{Prob(sift)}}{\text{Prob(sift)}_{\rm NT}} - 1\right| = 1.52\times10^{-3} \tag{19}$$

and

$$\left|\frac{\text{Prob(error)}}{\text{Prob(error)}_{\rm NT}} - 1\right| = 1.97\times10^{-7}, \tag{20}$$

showing that scintillation has indeed had a negligible influence on the sift and error probabilities.

Before moving on to the ground-to-satellite scenario, it is worth noting that the key-distribution secrecy of BB84 QKD depends on Prob(error | sift)—a quantity usually called the quantum bit-error rate (QBER)—being sufficiently small. In particular, the QBER provides an estimate of the information an eavesdropper may have obtained about the sifted bits, which, in turn, dictates the amount of privacy amplification required for Alice and Bob to distill a shared secret key. For the example given above we find that

$$\text{Prob(error | sift)}_{\rm NT} = 1.92\times10^{-2} \tag{21}$$

in the absence of turbulence, and we get

$$\left|\frac{\text{Prob(error | sift)}}{\text{Prob(error | sift)}_{\rm NT}} - 1\right| = 1.53\times10^{-3} \tag{22}$$

in the presence of worst-case scintillation. Thus worst-case scintillation on the satellite-to-ground path has virtually no effect on the QBER.

IV. GROUND-TO-SATELLITE SCENARIO

Now let us turn to the ground-to-satellite scenario. We continue to make the geometric assumptions that we employed for the satellite-to-ground case, namely that the ground terminal's diameter-D_G exit pupil comprises many turbulence coherence areas, and that the satellite's diameter-D_S entrance pupil lies well within a single turbulence coherence area. Here, however, it turns out that there are two cases worth considering: nonadaptive versus adaptive-optics transmitters. We start with the nonadaptive case using a collimated-beam transmitter.

A. Collimated-beam transmitter

In the absence of turbulence, a ground-based collimated-beam transmitter whose normalized spatial mode pattern is

$$\xi_o(\boldsymbol{\rho}) = \begin{cases} \sqrt{\dfrac{4}{\pi D_G^2}}, & \text{for } |\boldsymbol{\rho}| \leqslant D_G/2, \\ 0, & \text{otherwise}, \end{cases} \tag{23}$$

achieves $\gamma_{\rm NT}$ for its far-field power transfer to the satellite. In the presence of turbulence, this same collimated-beam transmitter yields $\gamma = \mu\mathcal{L}$ for its fractional power transfer, where

$$\mu = \left(\frac{D_S}{D_G\lambda L}\right)^2 \left| \int_{\boldsymbol{\rho}\leqslant D_G/2} d\boldsymbol{\rho}\, e^{\chi(\mathbf{0},\boldsymbol{\rho})+i\phi(\mathbf{0},\boldsymbol{\rho})} \right|^2. \tag{24}$$

In this expression, $\chi(\mathbf{0},\boldsymbol{\rho})$ and $\phi(\mathbf{0},\boldsymbol{\rho})$ are the log-amplitude and phase fluctuations imposed on the field received at transverse coordinate $\mathbf{0}$ in the $z = L$ plane from a point source at transverse coordinate $\boldsymbol{\rho}$ in the $z = 0$ plane. Atmospheric reciprocity [15] implies that this $\chi(\mathbf{0},\boldsymbol{\rho})$ and $\phi(\mathbf{0},\boldsymbol{\rho})$ can also be regarded as the log-amplitude and phase fluctuations imposed on the field received at transverse coordinate $\boldsymbol{\rho}$ in the $z = 0$ plane from a point source radiating from transverse coordinate $\mathbf{0}$ in the $z = L$ plane.

The average behavior of the preceding μ is well known (see, e.g., [11]). For our case, in which the ground terminal's exit pupil comprises many turbulence coherence areas, we can use the asymptotic result,

$$\langle\mu\rangle = \left(\frac{\pi D_T D_S}{4\lambda L}\right)^2, \tag{25}$$

where

$$D_T = 3.18\rho_0 \tag{26}$$

gives the effective (turbulence-limited) transmitter diameter in terms of the turbulence coherence length

$$\rho_0 = \left(2.91k^2 \int_0^L dz\, C_n^2(z)(1 - z/L)^{5/3}\right)^{-3/5}, \tag{27}$$

with $k = 2\pi/\lambda$ being the wave number at the laser wavelength, and $C_n^2(z)$ being the turbulence strength parameter along the propagation path from the ground terminal to the satellite. Note that this result, which was originally derived in the weak-perturbation (Rytov-approximation) regime, *is* valid in the strong-perturbation regime. More importantly, $D_T \ll D_G$, because we have assumed that the ground terminal's exit pupil comprises a large number of turbulence coherence areas. It follows that $\langle\mu\rangle \ll \mu_{\rm NT}$ for the collimated-beam (nonadaptive) ground-to-satellite transmitter. This is the well-known beam spread result, which has driven earth-space BB84 QKD designs to prefer satellite-to-ground operation, wherein $\langle\mu\rangle = \mu_{\rm NT}$ prevails [5], as we saw in Sec. III.

To complete our evaluation of the sift and error probabilities for the collimated-beam transmitter, we make use of the central limit theorem argument that implies μ will be exponentially distributed when the ground terminal's exit pupil contains a large number of turbulence coherence areas. Unlike the lognormal statistics that arose in Sec. III, the exponential distribution leads to simple closed-form results, i.e.,

$$\text{Prob(sift)} = \frac{\eta e^{-4\eta n_N}}{2}\left(\frac{n_S\langle\mu\rangle\mathcal{L}}{(1+\eta n_S\langle\mu\rangle\mathcal{L})^2} + \frac{4n_N}{1+\eta n_S\langle\mu\rangle\mathcal{L}}\right), \tag{28}$$

and

$$\text{Prob(error)} = \frac{\eta n_N e^{-4\eta n_N}}{1+\eta n_S\langle\mu\rangle\mathcal{L}}. \tag{29}$$

In seeking to assess the impact of scintillation on this nonadaptive-transmitter QKD system, it is unfair to compare these probabilities to the results from Eqs. (8) and (9), because those sift and error probabilities assume that there is no turbulence, whereas turbulence-induced beam spread—which is due primarily to the phase fluctuations $\phi(\mathbf{0},\boldsymbol{\rho})$—has a dramatic impact on the average ground-to-satellite power transfer even if there are no log-amplitude fluctuations, viz., $\chi(\mathbf{0},\boldsymbol{\rho}) = 0$. So, for our comparison case, we consider a ground-to-satellite link in which $p(\mu) = \delta(\mu - \langle\mu\rangle)$ with $\langle\mu\rangle$ given by the turbulence-limited result from Eq. (25). This no-scintillation (NS) case then has the following sift and error probabilities:

$$\text{Prob(sift)}_{\rm NS} = \eta(n_S\langle\mu\rangle\mathcal{L}/2 + 2n_N)e^{-\eta(n_S\langle\mu\rangle\mathcal{L}+4n_N)}, \tag{30}$$

and

$$\text{Prob(error)}_{\rm NS} = \eta n_N e^{-\eta(n_S\langle\mu\rangle\mathcal{L}+4n_N)}. \tag{31}$$

Figure 3 shows plots of $\text{Prob(sift)}_{\rm NS}$, $\text{Prob(error)}_{\rm NS}$, and $\text{Prob(error | sift)}_{\rm NS}$ versus $\langle\mu\rangle\mathcal{L}$. The n_S, n_N, and η values assumed are the same as were used in the satellite-to-ground example in Sec. III, viz., $n_S = 0.5$, $n_N = 5\times10^{-6}$, and $\eta = 0.5$. These curves are indistinguishable from similar plots for Prob(sift), Prob(error), and Prob(error | sift) because, over the range $10^{-4} \leqslant \langle\mu\rangle\mathcal{L} \leqslant 10^{-2}$, we have that

$$\max\left|\frac{\text{Prob(sift)}}{\text{Prob(sift)}_{\rm NS}} - 1\right| = 2.48\times10^{-3}, \tag{32}$$

$$\max\left|\frac{\text{Prob(error)}}{\text{Prob(error)}_{\rm NS}} - 1\right| = 3.11\times10^{-6}, \tag{33}$$

$$\max\left|\frac{\text{Prob(error | sift)}}{\text{Prob(error | sift)}_{\rm NS}} - 1\right| = 2.49\times10^{-3}, \tag{34}$$

when $n_S = 0.5$, $n_N = 5\times10^{-6}$, and $\eta = 0.5$. Once again we see virtually no effect from scintillation.

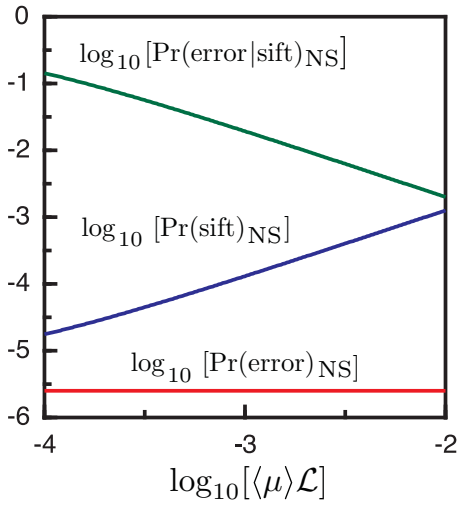

FIG. 3. (Color online) No-scintillation sift probability, error probability, and quantum bit-error rate plotted vs the logarithm of the average fractional power transfer, $\langle\mu\rangle\mathcal{L}$. These curves assume $n_S = 0.5$, $n_N = 5 \times 10^{-6}$, and $\eta = 0.5$.

B. Optimum adaptive-optics transmitter

For the far-field ground-to-satellite scenario we are considering, it is known that the optimum adaptive-optics transmitter—which perfectly adapts *both* the amplitude *and* the phase of the transmitter's spatial mode pattern to maximize the fractional power transfer—produces the following normalized spatial mode pattern [16]:

$$\xi(\boldsymbol{\rho}) = \begin{cases} \dfrac{e^{\chi(\mathbf{0},\boldsymbol{\rho})-i\phi(\mathbf{0},\boldsymbol{\rho})}}{\left(\displaystyle\int_{|\boldsymbol{\rho}|\leqslant D_G/2} d\boldsymbol{\rho}\, e^{2\chi(\mathbf{0},\boldsymbol{\rho})}\right)^{1/2}}, & \text{for } |\boldsymbol{\rho}| \leqslant D_G/2, \\ 0, & \text{otherwise.} \end{cases} \tag{35}$$

This transmitter achieves

$$\mu = \frac{\pi D_S^2}{4(\lambda L)^2} \int_{|\boldsymbol{\rho}|\leqslant D_G/2} d\boldsymbol{\rho}\, e^{2\chi(\mathbf{0},\boldsymbol{\rho})}, \tag{36}$$

because it is the reciprocity dual of the satellite-to-ground case. Hence the same considerations made in Sec. III show that scintillation has essentially no effect on the sift probability, error probability, and quantum bit-error rate of this system.

V. CONCLUSIONS

We have evaluated the sift probability, error probability, and quantum bit-error rate for satellite-to-ground and ground-to-satellite BB84 QKD when the ground terminal's entrance-exit pupil contains a large number of turbulence coherence areas, the satellite's entrance-exit pupil lies well within a single turbulence coherence area, and operation is deep into the far-field power-transfer regime. For reasonable choices of the average transmitted photon number, the average number of noise photons reaching each detector, and the quantum efficiency, we have found that scintillation has no appreciable effect on the aforementioned performance metrics. Two final questions are worth addressing. First, why is it that scintillation is so impotent here, when it has long been known to have a major impact on the error probabilities of uncoded laser communication systems? Second, would our results change were we to use the γ-γ distribution, instead of the lognormal distribution, for the satellite-to-ground scenario and the optimum adaptive-optics ground-to-satellite scenario? The reason for the disparity in scintillation effects is that laser communication systems are trying to operate at very low error probabilities, whereas the typical QBER of a free-space optical BB84 QKD system is a few percent. As a result, it is hard for even the most severe fading to change the QKD performance from what is achieved at the average value of the fractional power transfer. Consequently, we do not expect the results we reported for the lognormal distribution in Sec. III to be changed in any significant way if we did a similar calculation using the γ-γ distribution.

ACKNOWLEDGMENTS

This work was sponsored by the US Air Force under Air Force Contract No. FA8721-05-C-0002.

[1] J. H. Shapiro, Phys. Rev. A **67**, 022309 (2003).
[2] J. H. Shapiro, Appl. Opt. **13**, 2614 (1974).
[3] Calling a BB84 QKD system that operates over a line-of-sight atmospheric path a "free-space" implementation is common practice but is nonetheless a misnomer because free-space propagation implies that the propagation is through vacuum. Nevertheless, we use the common terminology.
[4] A notable exception in this regard is G. Gilbert and M. Hamrick, e-print arXiv:quant-ph/0009027v5, which draws upon well-established statistical results for the phase and log-amplitude fluctuations produced by propagation through turbulence but does not directly address the resulting QKD sift and error probabilities.
[5] M. Aspelmeyer, T. Jennewein, M. Pfennigbauer, W. R. Leeb, and A. Zeilinger, IEEE J. Sel. Top. Quantum Electron. **9**, 1541 (2003).
[6] The γ-γ distribution provides a more accurate representation of scintillation statistics [see L. C. Andrews, R. L. Phillips, and C. Y. Hopen, *Laser Beam Scintillation with Applications* (SPIE, Bellingham, WA, 2001), Chap. 3], but its aperture-averaged behavior is less convenient to work with than the lognormal case, for which aperture-averaged scintillation tends to retain its lognormal character. As explained in Sec. V, we do not believe that γ-γ scintillation leads to a more severe impact on the sift and error probabilities.
[7] We 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.
[8] 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.

[9] Note that γ is really a fractional energy transfer. However, because our QKD system employs pulse durations that are much longer than the ∼picosecond-duration multipath spread and much shorter than the ∼millisecond coherence time of the turbulent atmosphere, the atmosphere does not disturb the normalized shape of the transmitted pulse. Under these conditions fractional energy transfer is the same as fractional (average or peak) power transfer.

[10] The far-field power-transfer regime is defined by the condition $(\pi D_G D_S/4\lambda L)^2 \ll 1$.

[11] J. H. Shapiro, in *Laser Beam Propagation in the Atmosphere*, edited by J. W. Strohbehn (Springer-Verlag, Berlin, 1978), Chap. 6.

[12] Of course, opening up the receiver's field of view to accommodate turbulence-induced angular spread increases the amount of background light collected by that receiver.

[13] R. L. Mitchell, J. Opt. Soc. Am. **58**, 1267 (1968).

[14] Strictly speaking, the lognormal model cannot be correct, as it assigns nonzero probability to the impossible event $\mu > 1$. However, because $\mu_{\rm NT} \ll 1$ holds in far-field power transfer and $\langle e^{2u} \rangle = 1$, the likelihood that the lognormal distribution assigns to this aphysical $\mu > 1$ event is inconsequentially small. A similar observation applies to the exponential fading statistics that arise in the ground-to-satellite case when a nonadaptive (collimated-beam) transmitter is employed.

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

[16] J. H. Shapiro, IEEE Trans. Commun. Technol. **19**, 410 (1971).