Scintillation discriminator improves free-space quantum key distribution

Feng Tang (唐 峰) and Bing Zhu (朱 冰)*

Department of Electronic Engineering and Information Science,
University of Science and Technology of China, Hefei 230026, China
**Corresponding author: zbing@ustc.edu.cn*

Received March 26, 2013; accepted June 28, 2013; posted online September 3, 2013

We present an analysis of the impact of afluctuating-loss channel on free-space quantum key distribution (QKD). Considering the characteristics of the fluctuating-loss channel, a scintillation discriminator that acts according to the information of instant channel loss is proposed to help improve the performance of a free-space QKD system, which suffers from the influence of atmospheric turbulence. Theoretical and numerical results show that this discriminator is a useful tool for increasing secure key rates, especially for long-range free-space QKD.

OCIS codes: 010.1330, 060.5565, 270.5568.
doi: 10.3788/COL201311.090101.

In recent years, quantum key distribution (QKD) has attracted significant research attention because it offers absolute security based on the fundamental laws of physics[1,2]. QKD is currently the most promising implementation method based on quantum information theory. Two types of QKD implementations are available according to the quantum transmission medium used: QKD based on optical fibers and free-space QKD. For free-space links and long-range free-space QKD between orbit satellites and ground stations, quantum signals are subject to various environmental distortions. Thus, the channel characteristics of the atmosphere are important considerations for a practical free-space QKD system.

When a laser beam propagates through the earth's atmosphere, it encounters a variety of deleterious effects relevant to phase and amplitude distortions due to random refractive-index variations resulting from atmospheric turbulence[3]. These disturbances cause instability of atmospheric losses and permanent fluctuation in turbulence channels, which are referred to as fluctuating-loss channels[4]. The impact of turbulence-induced scintillation usually plays an important role in noise in optical communications[5], wherein deep, long-lived scintillation fades, ultimately limiting the system performance in high-reliability operations. Shapiro[6] demonstrated that the related noise arising from propagation through atmospheric turbulence does not significantly affect the sift and error probabilities of a free-space QKD system that employs weak coherent pulses with decoy states. In other words, almost no difference is observed between a static channel and a fluctuating-loss channel so long as the average channel loss remains the same[7], since fluctuations in quantum bit error rate (QBER) induced by variations in channel loss are averaged over time. As only the average QBER is applied to the QKD system, it has virtually no influence on the process of generating a final secure key. Erven *et al.*[8] showed that the total secret key generated in a QKD system can be significantly increased by throwing away data blocks where the signal-to-noise ratio (SNR) is lower than a certain threshold. In their work, atmospheric turbulence fluctuations in free-space links were measured using entangled photons. Capraro *et al.*[9] also suggested that the SNR of a quantum signal can be improved by probing the transmission of the channel by means of a classical signal and acquiring only single-photon signals when the instantaneous transmission of the channel is above a given threshold. Both studies indicate that the exploitation of turbulence can be used as an improvement technique for free-space QKD.

In this letter, unlike previous key generation calculations presented in Refs. [7,8], the fluctuating QBER is directly addressed to the resulting secure key rate, which is the principal figure-of-merit ofa QKD system, before averaging. Such fluctuations are useful for improving the key rate of a free-space QKD system. A scintillation-based key data grouping scheme that takes advantage of the fluctuating-loss channel is then proposed. The rest of this letter is organized as follows: firstly, we calculate the secure key rate of a free-space QKD system under a fluctuating-loss channel. The scintillation-based key data grouping scheme, which introduces a discriminator acting according to the information of channel loss to the key process, is then described to increase the secure key rate of QKD. Finally, the efficiency of the proposed scheme is evaluated in a virtual optical scintillation scenario of 20 km by employing the numerical simulation method of multiple phase screens.

As shown in Fig. 1, an additional reference link utilizing periodic bright light pulses is employed to perform channel loss monitoring. The instantaneous atmospheric information obtained from this classical link is used to

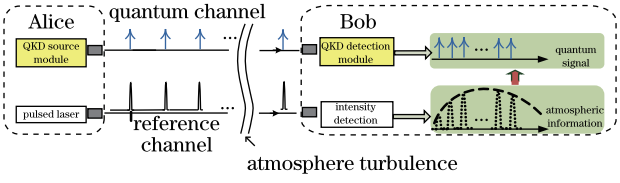

Fig. 1. (Color online) Schematic of QKD system with an additional reference link.

denote the instant QBER and fulfill the task of signal data grouping. In the present study, the secure key resolving model of one-decoy protocol from Ref. [10] is adopted. The sender, typically called Alice, transmits the weak coherent signal pulses with average photon number μ to the recipient, typically referred to as Bob. Let η denote the overall transmittance, including average channel loss, the internal transmittance in Bob, and the detector efficiency. $\eta_{\rm ato}$ represents the normalized atmospheric transmittance due to the fluctuating channel loss. Thus, the instantaneous channel transmittance can be expressed as $\eta\eta_{\rm ato}$. At Bob's side, the conditional probability of detecting a photon event in a pulse is given by the value of $\eta_{\rm ato}$:

$$\Pr(\text{event}|\eta_{\rm ato}) = Q_\mu = Y_0 + 1 - \mathrm{e}^{-\eta\eta_{\rm ato}\mu}, \quad (1)$$

and the conditional QBER is given by

$$\Pr(\text{error}|\eta_{\rm ato}) = E_\mu = \frac{e_0 Y_0 + e_{\rm det}(1 - \mathrm{e}^{-\eta\eta_{\rm ato}\mu})}{Q_\mu}, \quad (2)$$

where Y_0 is the probability of detecting a noise event in a pulse, $e_{\rm det}$ characterizes the probability that a signal photon hits the wrong detector, and $e_0 = 0.5$ for the BB84 protocol. Y_0, which represents the receiving noise level of a QKD system, is obviously not affected by atmospheric turbulence and remains constant. $\eta_{\rm ato}$, upon which the QBER fluctuates, is added to represent the effect of scintillation in a turbulence channel. Thus, the asymptotic key rate per transmitted pulse (R) conditionally on knowledge of $\eta_{\rm ato}$ is given by

$$R = q\{-Q_\mu f(E_\mu) H_2(E_\mu) + Q_1[1 - H_2(e_1)]\}, \quad (3)$$

where $q = 0.5$ for the BB84 protocol, $H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary entropy function, $f(E_\mu) = 1.22$ is the error correction efficiency for practical error correction codes, and Q_1 and e_1 are the respective estimated gain and error rates for single-photon pulses; Q_1 and e_1 can be calculated from Section D of Ref. [10] to obtain the final key rate shown in Eq. (3).

To derive the unconditional secure key rate, the results of Eq. (3) must be averaged using the probability distribution of normalized channel loss $P(\eta_{\rm ato})$. For long-range light transmission in the regime of weak fluctuations and strong losses, the probability distribution model of the turbulence-induced loss is generally accepted to be log-normally distributed[11]. This behavior has also been verified through experiments on the transmission ofa single photon level[9,12]. The lognormal distribution of the normalized atmospheric transmittance can be expressed as[11]

$$p(\eta_{\rm ato}) = \frac{1}{\sigma_I \eta_{\rm ato}\sqrt{2\pi}} \exp\left\{-\frac{1}{2\sigma_I^2}\left[\ln(\eta_{\rm ato}) + \frac{\sigma_I^2}{2}\right]^2\right\}, \quad \eta_{\rm ato} > 0, \quad (4)$$

Table 1. Parameters for Key Rate Calculation

Signal State μ (/pulse)	Decoy State ν (/pulse)	Noise Level Y_0 (/pulse)	System Error $e_{\rm det}$ (%)
0.6	0.2	1.25×10^{-5}	1

where $\sigma_{\rm I}^2$ is the scintillation index representing the strength of the scintillation effect. Therefore,the unconditional secure key rate can be expressed as

$$R_{\rm ato} = \int_0^\infty R(\eta_{\rm ato}) p(\eta_{\rm ato}) \mathrm{d}\eta_{\rm ato}, \quad (5)$$

where $R_{\rm ato}$ is calculated under different scintillation conditions described by the scintillation index. The parameters are listed in Table 1.

Figure 2 compares the key rates based on average QBER versus fluctuating QBER. Line 1 represents the secure key rate with average QBER, wherein no difference is observed in the key generation rates for various scintillation indices so long as the average channel loss is the same. Lines 2 to 4 represent the key rates calculated from Eq. (5) under different magnitudes of scintillation. The results show that directly addressing fluctuations in atmospheric transmittance to key generation in a fluctuating-loss channel is helpful. Taking the instantaneous key rate and averaging over the channel loss, rather than the key rate of the average channel loss and QBER, promotes the efficiency of the key generation algorithm. Therefore, more keys can be earned by utilizing the instant information obtained from fluctuating QBER. For a given noise level $Y_0 = 1.25 \times 10^{-5}$, the key rate may be significantly increased when the total loss is above 34 dB, which indicates that considering the fluctuating QBER, rather than the average QBER is valuable, especially for long-range free-space QKD. This comparison prompts us to design a free-space QKD system that reacts with variations in channel loss in real-time, upon which our scintillation-based technique is based.

Typically, five steps are carried out to generate a secret key in QKD: authentication, single photon transmission, sifting, error correction, and privacy amplification[13]. Once Alice and Bob complete single-photon transmissions, they need to collect a sufficient number of qubits to move on to the next step because a single qubit cannot be transformed into a key. Before qubits are handled for error removal, incoming signals stay in a "key pool" to wait, as shown in Fig. 3. For long-range free-space QKD, the waiting time is approximately 1-s timescale because of the low key rate, since more time is needed to prepare a bit sequence. Compared with the frequency of temporal scintillation, which is normally about several hundred Hz, fluctuation sin QBER in a bit sequence are averaged. Thus, the QKD system cannot "read" turbulence-induced scintillation. Only the average QBER is applied to the following phases of the QKD protocol, such as reconciliation and privacy amplification.

To take advantage of optical scintillation, in Fig. 3, a scintillation discriminator acting according to the information of channel loss is introduced to the QKD data procedure steps. The qubits in the key pool are re-sorted by the discriminator according to the corresponding atmospheric transmittance rather than the arrival time. In this way, QBER of the forming bit strings differ from each other. Since bits are gathered by the information of channel loss, fluctuations in QBER in bit sequences will not be averaged by time, and the connection between the QKD system and the fluctuating-loss channel may be built. From the key processing point of view, the error correction efficiency is improved by distinguishing

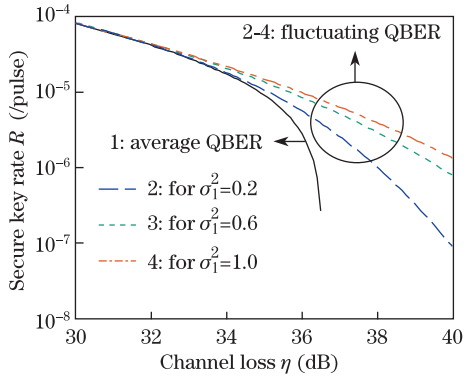

Fig. 2. (Color online) Secure key rates obtained under different scintillation conditions.

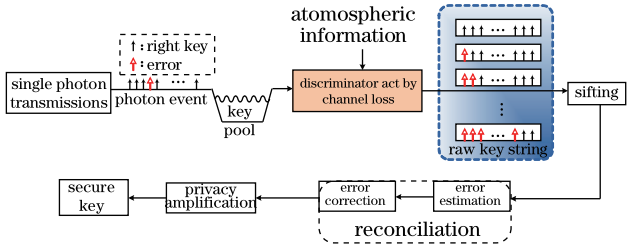

Fig. 3. (Color online) Data acquisition illustration of the proposed BCS method.

fluctuation sin QBER in the qubit sequences. Especially for a free-space link with high losses, bit strings with QBER values higher than the secure threshold are automatically blocked by the error correction algorithm to significantly increase the total number of secure keys.

To evaluate the performance of the proposed scintillation-based method in a practical scenario, the multiple phase screen method[14] is employed to simulate a beam propagating in a turbulent atmosphere. A collimated Gaussian beam propagating through a distance of 20 km is simulated; here, the refractive-index structure parameter C_n^2 is constant along the entire beam path. As shown in Fig. 4, the propagation distance is evenly divided into 11 layers by phase screens. Propagation across a layer is split into two parts-firstly, it propagates through Δz in the absence of turbulence, after which it passes through a phase screen that represents the effect of turbulence. A phase screen, which is there alization of atmospheric phase perturbation, is generated with the spectral domain retrieval algorithm involving the parameter C_n^2. After generating phase screens, the beam is allowed to travel through the layered model of the atmosphere and reach the receiving plane. In the receiving plane, the intensity of the beam in the diameter of the receiver is accumulated and compared with the original transmitting energy. This way, the instantaneous channel loss of one transmission is simulated.

The statistic of channel loss is firstly derived by repeating the transmission simulation many times (1000 times). The simulation parameters are listed in Table 2. Figure 5 shows the results of the simulated distribution of normalized channel loss. Because of the aperture averaging effect, the scintillation index obtained with a collecting aperture (D = 30 cm) is smaller than that obtained by a "point" aperture (D = 0). As the scintillation index increases, the distribution also changes from a lognormal model to a negative-exponential model. The simulation results agree well with optical scintillation theory.

The efficiency of our scintillation-based method is then verified by the channel loss data obtained from the multiple phase screen method. For practical applications, infinitely subdividing the key datais unrealistic. Thus, the discriminatormust identify atmospheric transmittance values from only a few classes. The first class is the key data, of which the estimation of QBER is above the secure threshold (typically 11%). The rest of the key data can be divided into N classes according to the measured channel loss:

$$\begin{aligned}&\text{High QBER group: } \eta_i \in [0, \eta_{\text{thr}}];\\ &\text{Other QBER group:}\\ &\eta_i \in \underbrace{[\eta_{\text{thr}}, \eta_1], \quad [\eta_1, \eta_2], \quad \cdots \quad [\eta_{N-1}, \eta_N]}_{N \text{ classes}},\end{aligned} \tag{6}$$

where η_i is the normalized atmospheric transmittance for each signal pulse, and η_{thr} is obtained from Eq. (2) by setting a secure QBER threshold. The simulation is run 1 000 times and 1 000 measurements of channel loss are obtained. The total secure key rate for the N classes scheme is

$$R_N = \frac{r_1 \cdot n_1 + r_2 \cdot n_2 + \cdots + r_N \cdot n_N}{n_0 + n_1 + n_2 + \cdots + n_N}, \tag{7}$$

where r and n respectively represent the key rate and simulation number with different classes of QBER values. n_0 is the number of the high QBER group and the corresponding key rate $r_0 = 0$ is omitted. To evaluate

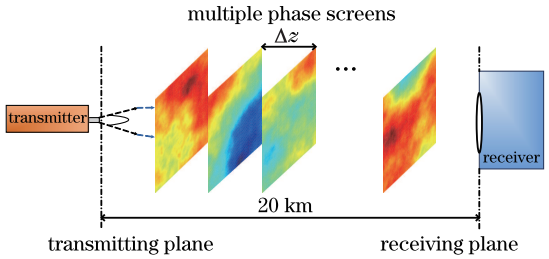

Fig. 4. (Color online) Schematic of the phase screen method for modeling beam propagation in a turbulent atmosphere.

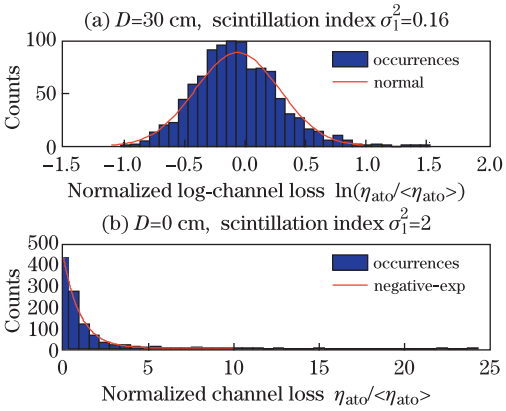

Fig. 5. (Color online) Simulated distribution of normalized channel loss.

Table 2. Parameters for Beam Propagation Simulation

Signal Wavelength (nm)	Transmitter Diameter (cm)	Receiving Diameter (cm)	Transmission Distance (km)	Turbulence Strength ($m^{-2/3}$)
650	5	30	20	5×10^{-16}

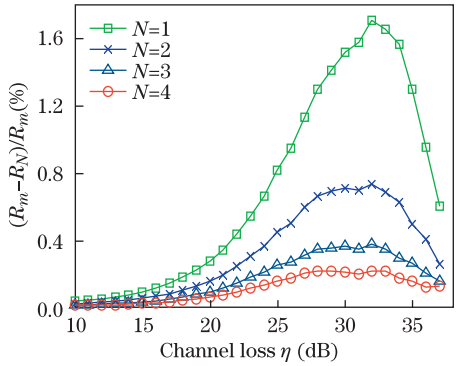

Fig. 6. (Color online) Key rate comparison at different values of N.

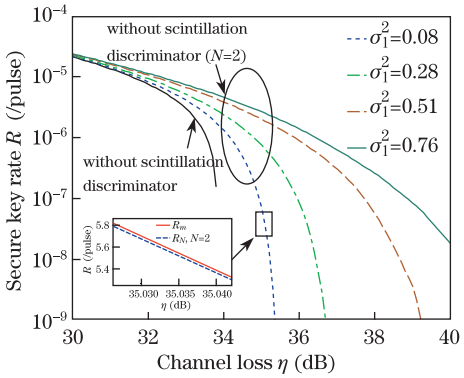

Fig. 7. (Color online) Numerical simulation of the $N = 2$ grouping scheme.

the influence of the number N, the mean key rate R_m for each simulated data is calculated to represent an infinite grouping scenario in this simulation experiment. Figure 6 shows that no more than a 2% decrement is observed even with $N = 1$ compared with R_m under different channel losses. Therefore, the key data can be simply re-sorted into 2 to 3 classes to implement the scintillation-based QBER grouping scheme for practical purposes.

The performance of the $N = 2$ grouping scheme under different scintillation indices turbulence is shown in Fig. 7. A detailed drawing with R_m is also shown in the figure for comparison with the R_N grouping scheme. Simulation parameters are indicated in Tables 1 and 2, but the turbulence strength C_n^2 is changed to simulate the circumstance of varied σ_I^2. The scintillation index is calculated from statistical parameters of the channel loss data. The efficiency of the scintillation-based grouping scheme increases with increasing scintillation index when the average channel loss is constant. Considerable improvements may be observed compared with the original key rates obtained without introduction of the discriminator. Especially for long-range free-space QKD, the proposed method can greatly increase secure key rates and extend the secure distance. Such results may be obtained because more signals from the high QBER group are distinguished from the original key data and automatically discarded by the secure key generation process.

In conclusion, the effects of fluctuating loss induced by optical turbulence on free-space QKD are analyzed. Results show that the QKD system can be improved by introducing a discriminator that acts according to the information of channel loss to key processing. The present scintillation-based data grouping scheme serves asa useful tool for increasing secure key rates in the case of fluctuating loss, especially for long-range free-space QKD. The efficiency of this scheme is verified by employing the multiple-phase screen method.

This work was supported by the "Hundred Talents Program" of Chinese Academy of Sciences.

References

1. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus, and M. Peev, Rev. Mod. Phys. **81,** 1301 (2009).
2. Z. Zhao, Y. Luo, Z. Zhao, and H. Long, Chin. Opt. Lett. **9,** 032702 (2011).
3. J. W. Strohbehn, *Laser Beam Propagation in the Atmosphere* (Springer, Berlin / Heidelberg, 1978).
4. A. Semenov and W. Vogel, Phys. Rev. A **80,** 021802 (2009).
5. Y. Zhao, D. Xu, and X. Zhong, Chin. Opt. Lett. **9,** 110602 (2011).
6. J. H. Shapiro, Phys. Rev. A **84,** 032340 (2011).
7. E. Meyer-Scott, Z. Yan, A. Macdonald, J. P. Bourgoin, H. Hubel, and T. Jennewein, Phys. Rev. A **84,** 062326 (2011).
8. C. Erven, B. Heim, E. Meyer-Scott, J. P. Bourgoin, R. Laflamme, G. Weihs, and T. Jennewein, New J. Phys. **14,** 123018 (2012).
9. I. Carpraro, A. Tomaello, A. Dall'Arche, F. Gerlin, R. Ursin, G. Vallone, and P. Villoresi, Phys. Rev. Lett. **109,** 200502 (2012).
10. X. Ma, B. Qi, Y. Zhao, and H. K. Lo, Phys. Rev. A **72,** 012326 (2005).
11. L. C. Andrews, R. L. Phillips, and C. Y. Hopen, *Laser Beam Scintillation with Applications* (SPIE Press, 2001).
12. P. W. Milonni, J. H. Carter, C. G. Peterson, and R. J. Hughes, J. Opt. B Quantum Semiclass. Opt. **6,** S742 (2004).
13. J. E. Nordholt, R. J. Hughes, G. L. Morgan, C. G. Peterson, and C. C. Wipf, Proc. SPIE **4635,** 116 (2002).
14. R. Frehlich, Appl. Opt. **39,** 393 (2000).