CHIN. PHYS. LETT. Vol. 33, No. 12 (2016) 120302

Decoy State Quantum Key Distribution via Beam-Wandering Modeled Atmosphere Channel *

Sheng-Li Zhang(张胜利)[1,2**], Chen-Hui Jin(金晨辉)[1], Jian-Sheng Guo(郭建胜)[1], Jian-Hong Shi(史建红)[1], Xu-Bo Zou(邹旭波)[2], Guang-Can Guo(郭光灿)[2]

[1]*The PLA Information Engineering University, Zhengzhou 450004*

[2]*Key Laboratory of Quantum information, University of Science and Technology of China, Hefei 230026*

(Received 22 August 2016)

We investigate the decoy state quantum key distribution via the atmosphere channels. We consider the efficient decoy state method with one-signal state and two-decoy states. Our results show that the decoy state method works even in the channels with fluctuating transmittance. Nevertheless, the key generation rate will be dramatically decreased by atmosphere turbulence, which sheds more light on the characterization of atmosphere turbulence in realistic free-space based quantum key distributions.

PACS: 03.67.Hk, 42.50.Ex, 03.67.Hk, 03.67.Mn DOI: 10.1088/0256-307X/33/12/120302

Quantum key distribution (QKD) is an efficient and physically secure method for establishing a random and private key between distant participants, Alice and Bob. Since its first proposal in 1984,[1] the Bennet–Brassard-84(BB84) quantum key distribution protocol has attracted a great deal of attention. The record of the distance of experimental quantum key distribution has been rapidly updated from 32 cm in 1989,[2] 125 km in 2004,[3] 200 km in 2010,[4] to 400 km in 2016.[5] In all practical implementations of the BB84 protocol, key elements are encoded by the single photon and photon loss is one of the most important factors that limits the key generation rate of practical key distributions. However, all analyses right now assume that the loss of channel is fixed, which is far too idealized.

To further extend the length of quantum channel and to implement the global quantum key distribution, the quantum link in free-space connecting satellite and ground stations is a promising quantum channel. Recent theories and experiments have proved the feasibility of single photon quantum communication over 1500 km.[6] The quantum channel in free space is always filled with atmosphere turbulence, which is one of the inevitable problems we should be concerned about. In this study, we give an investigation of quantum key distribution in the presence of atmospherical turbulence. We consider the efficient decoy state method for the weak coherent state and we use the key generation rate per photon emission as a figure of merit to evaluate the performance of quantum key distribution. Our results are based on the beam-wandering model of atmosphere turbulence, which fits very well in the weak turbulence condition. Numerical results show that the method of one-signal and two-decoy states still works effectively in a channel with fluctuating transmittance. Nevertheless, the atmosphere turbulence will dramatically decrease the secure key generation rate, which sheds light on the importance of characterization of atmosphere turbulence in free space quantum key distribution.

Unlike the traditional key distribution protocol,[7] the security of quantum key distribution, such as the BB84 protocol, is unconditional security which is based on the Heisenberg uncertainty principle[8] and non-cloning theorem in quantum information science.[9] The faithful implementation of the BB84 protocol requires a single photon state which is impossible even with the state-of-the-art single photon technique.[10] One convenient implementation of QKD always utilizes the attenuated weak coherent state (WCS) instead.[2,3] For the WCS, particularly if the average photon number is small ($\langle n\rangle = 0.1$), the multi-photon proportion is greatly suppressed: multi-probability scales as $p_{\rm multi} = 0.0046$.

Although extremely small, the multi-photon proportion is still comparable with the gain of single photon emission in long distance quantum communication. This could open the loophole of a photon number splitting attack which reduces the unconditional security of realistic key distribution within 20 km.[11] The relevant security analysis can be obtained from the well-known Gottesman–Lo–Lütkenhaus–Preskill (GLLP) formula[12]

$$R \geq \frac{1}{2}Q_\mu\Big\{-f(E_\mu)H(E_\mu) + (1-\Delta)\Big[1-H\Big(\frac{E_\mu}{1-\Delta}\Big)\Big]\Big\}, \quad (1)$$

where $\Delta = p_{\rm multi}/Q_\mu$, Q_μ is the gain defined as the number of Bob's detector counts over the number of the signal Alice transmitted on condition that Alice and Bob are utilizing the same basis in the BB84 protocol, and $f(E_\mu)$ is the efficiency of key reconciliation.[13]

The decoy state method[14–16] is a novel and efficient method for increasing the precision of estimation

*Supported by the National Natural Science Foundation of China under Grant Nos 11574400, U1304613, 11204197, 11204379 and 11074244, the National Basic Research Program of China under Grant No 2011CBA00200, and the Doctor Foundation of the Ministry of Education of China under Grant No 20113402110059.

**Corresponding author. Email: victory8@mail.ustc.edu.cn

© 2016 Chinese Physical Society and IOP Publishing Ltd

of single photon gain Q_1. Moreover, the decoy state also provides an additional tool for distinguishing the error rate contributed by single photon e_1 and few photon e_m. Thus the practical secure key generation rate is greatly improved even in the presence of a photon number splitting attack. The secure key rate for a decoy state is given by

$$R_{\rm decoy} = \frac{1}{2}\{-Q_\mu f(E_\mu)H(E_\mu) + Q_1(1-H(e_1))\}. \quad (2)$$

The decoy state method can be easily implemented with coherent states of different average photon numbers. The simplest decoy state quantum key distribution scheme consists of one signal state (coherent state with average photon number μ) and two decoy states (with average photon numbers ν_1 and ν_2). The signal state and the decoy state have the same physical property, except for the average photon number. Let the average photon numbers of the signal state, and decoy states be μ, ν_1 and ν_2 such that

$$0 \le \nu_2 \le \nu_1, \quad \nu_1 + \nu_2 < \mu < 1. \quad (3)$$

The total counts for the signal state and the decoy state can be given by

$$Q_\mu = \sum_n Y_n P(\mu, n), \quad (4)$$

$$Q_{\nu_1} = \sum_n Y_n P(\nu_1, n), \quad (5)$$

$$Q_{\nu_2} = \sum_n Y_n P(\nu_2, n), \quad (6)$$

where $P(\mu,n) = e^{-\mu}\mu^n/n!$ ($P(\nu,n) = e^{-\nu}\nu^n/n!$) denotes the probability that each signal (decoy) state photon pulse contains exactly n photons. The single photon gain can then be given by

$$Q_1 = P(\mu,1)Y_1^{\rm L}, \quad (7)$$

with $Y_1^{\rm L}$ given by[17]

$$Y_1^{\rm L} = \frac{\mu}{\mu\nu_1 - \mu\nu_2 - \nu_1^2 + \nu_2^2} \times \left(Q_{\nu_1}e^{\nu_1} - Q_{\nu_2}e^{\nu_2} - \frac{\nu_1^2 - \nu_2^2}{\mu^2}Q_\mu e^\mu\right). \quad (8)$$

The single photon error rate e_1 is the most important and can be estimated with the help of the decoy state[18]

$$e_1 \le e_1^{\rm U} = \frac{EQ_{\nu_1}e^{\nu_1} - EQ_{\nu_2}e^{\nu_2}}{(\nu_1 - \nu_2)Y_1^{\rm L}}, \quad (9)$$

with e_n and $EQ_\nu = \sum_n Y_n e_n P(\nu,n)$ being the error rate contributed by the n-photon pulse and the average error rate of the decoy state ν, respectively. With Eqs. (2) and (7)–(9), the secure key generation rate can be estimated. Theoretic results further show that the decoy state method can improve the distance of secure quantum key distribution up to 200 km, corresponding to the photon loss of 40 dB in the standard single mode communication fiber (1550 nm).[19]

Here we introduce the beam wandering-model of atmosphere turbulence. Actually, many models for atmosphere turbulence have been proposed and the beam-wandering model fits quite well under the weak turbulence condition. As shown in Bob's receiving apparatus in Fig. 1(a) and the x–y plot in Fig. 1(b), atmosphere turbulence will cause a deflection distance r between the beam spot center (solid circle, radius W) and the detector aperture center (dotted circle, radius a_2). This means that not all the photons arriving at the detecting plane will be detected. This equivalates to a beam splitter of transmittance[20]

$$T = T^* \exp\left[-\left(\frac{r}{R}\right)^\lambda\right], \quad (10)$$

with $T^* = 1 - \exp[-2\tau^2]$, $\tau = a_2/W$ and

$$\lambda = \frac{8\tau^2\exp[-4\tau^2]I_1(4\tau^2)}{1-\exp[-4\tau^2]I_0(4\tau^2)} \Big/ \ln\left(\frac{2T^*}{1-\exp[-4\tau^2]I_0(4\tau^2)}\right),$$
$$R = a_2\left[\ln\left(\frac{2T^*}{1-\exp[-4\tau^2]I_0(4\tau^2)}\right)\right]^{-1/\lambda}, \quad (11)$$

where $I_n(x)$ is the modified Bessel function of order n, and a_2 is the radius of the aperture of detector.

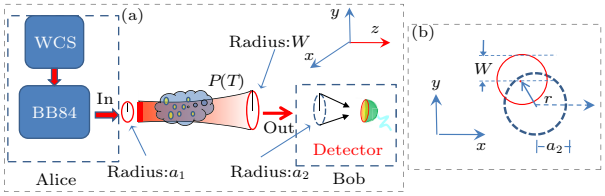

Fig. 1. (Color online) (a) Implementation of the BB84 protocol via the atmospheric turbulent channel. WCS represents the weak coherent state. The atmosphere channel is modeled by a beam splitter of transmittance T, with T being a random variable obeying probability distribution $P(T)$. Due to atmosphere turbulence, the beam spot center and the detection aperture center will be displaced by r in Bob's detector plane. Lenses for transmitting and gathering light signals are assumed to be a_1 and a_2. (b) Geometric relation between the beam spot (solid circle with radius W) and the detector aperture center (dotted circle with radius a_2) at the receiver plane.

Influenced by random turbulence, the deflection distance r is not fixed, it varies permanently. Thus the transmittance T is a random variable. This happens to be the biggest distinction between the turbulent channel and the standard attenuating channel with fixed transmittance. To a good approximation, the deflection distance r follows the Rice approximation with parameter $d = \langle r\rangle$ and variance σ.[21–23] The probability distribution of transmittance (PDTC)

then follows

$$P(T)=\frac{R^2}{\sigma^2\lambda T}\Big(\ln\frac{T^*}{T}\Big)^{\frac{2}{\lambda}-1}I_0\Big[\frac{Rd}{\sigma^2}\Big(\ln\frac{T^*}{T})^{1/\lambda}\Big]\exp\Big\{-\frac{1}{2\sigma^2}\Big[R^2\Big(\ln\frac{T^*}{T}\Big)^{\frac{2}{\lambda}}+d^2\Big]\Big\}. \quad (12)$$

Particularly, if the beam fluctuates around the aperture center, $d=0$, the distribution reduces to the log-negative Wibull function, $P(T)=\frac{R^2}{\sigma^2\lambda T}[\ln\frac{T^*}{T}]^{\frac{2}{\lambda}-1}\exp[-\frac{1}{2\sigma^2}R^2(\ln\frac{T^*}{T})^{\frac{2}{\lambda}}]$.

To evaluate the performance of the decoy state QKD, we should consider the theoretic gain of n-photon pulse. Suppose an n-photon state is prepared by the photon source in Alice's laboratory. The n-photon pulse will suffer from photon loss of three phases: (1) atmosphere channel with probabilistic transmittance T, (2) the photon loss in Bob's receiving device, (3) the photon loss in non-unit quantum efficiency of the single photon detector. All the three phases can be modeled with beam splitters of transmittance T, $\eta_{\rm Bob}$ and $\eta_{\rm det}$, respectively. The optic path is depicted in Fig. 2. A thermal state $\rho_{\rm th}=\sum_{k=0}^{\infty}\frac{n_{\rm th}^k}{(n_{\rm th}+1)^{k+1}}|k\rangle\langle k|$ with the average photon number $n_{\rm th}$ is fed into the other port of beam splitter $\rm BS_1$, simulating the effect of background noise. For the n-photon input, the total detection efficiency is given by

$$\begin{aligned}Y_n^{\rm atmo}&=\int P(T)P_{\rm succ}(n|T)dT\\&=1-\int P(T)\langle 0|\rho_{\rm A}^{\rm reduce}|0\rangle dT,\end{aligned} \quad (13)$$

with $\rho_{\rm A}^{\rm reduce}={\rm Tr}_{\rm BCD}[\rho_{\rm ABCD}]$ and $\rho_{\rm ABCD}=U_{\rm BS_3}U_{\rm BS_2}U_{\rm BS_1}(|n\rangle\langle n|\otimes\rho_{\rm th}\otimes|0\rangle_{\rm CD}\langle 0|)U_{\rm BS_1}^{\dagger}U_{\rm BS_2}^{\dagger}U_{\rm BS_3}^{\dagger}$ and $U_{\rm BS}(\eta)=\exp[\arctan\sqrt{(1-\eta)/\eta}(ab^{\dagger}-a^{\dagger}b)]$ being the unitary operator for a beam splitter with transmittance η. After some lengthy while not very interesting algebra, one obtains

$$\begin{aligned}\langle 0|\rho_{\rm A}^{\rm reduce}|0\rangle=&\frac{1}{n_{\rm th}+1}\sum_{m,p=0}^{\infty}\sum_{k,k'=0}^{n}\sum_{l,l'=0}^{m}\\&\times\delta_{n-k+l,p}\delta_{k-l,k'-l'}\xi_{n,m,k,l}\xi_{n,m,k',l'}\\&\times(1-\eta_{\rm Bob}\eta_{\rm det})^p\Big(\frac{n_{\rm th}}{n_{\rm th}+1}\Big)^m,\end{aligned} \quad (14)$$

with $\xi_{n,m,k,l}=\sqrt{\binom{n}{k}\binom{n-k+l}{l}\binom{m}{l}\binom{m+k-l}{k}}(-1)^l\cdot T^{\frac{m+n-k-l}{2}}(1-T)^{\frac{k+l}{2}}$.

Particularly, if the background noise vanishes, i.e., $n_{\rm th}=0$, one obtains that

$$\langle 0|\rho_{\rm A,vacuum}^{\rm reduce}|0\rangle=(1-T\eta_{\rm Bob}\eta_{\rm det})^n. \quad (15)$$

Since the atmosphere channel will never affect the photon emitting source, the photon number distribution of the signal state μ and the decoy state ν_1,ν_2 is still the Poisson distribution. Thus the inequalities for estimation of $Y_1^{\rm L}$ in Eq. (8) and $e_1^{\rm U}$ in Eq. (9) still holds and one can use Eq. (2) to evaluate the performance of QKD in atmosphere channels. For the experimental parameters, we consider the typical free-space quantum key distribution where two telescopes of the same size $a_1=a_2$ are utilized for the photon emission and photon detection. The variance σ and beam spot size W in Fig. 1 are determined by the atmosphere index-of-reflection structure constant C_n^2. Assuming the simplest cases where the coefficient C_n^2 is constant along the path z, the variance in the detecting plane is given by $\sigma^2=1.305C_n^2(2W_0)^{-1/3}L^3$. Influenced by the atmosphere turbulence, the beam size in the detecting plane will be widened to[24]

$$W=\sqrt{W_0^2+2\Big(\frac{L\lambda_0}{\pi r_0}\Big)^2}, \quad (16)$$

where λ_0 is the wavelength, and $r_0=[0.5476(\frac{2\pi}{\lambda_0})^2C_n^2L]^{-3/5}$ is the coherent length. For typical quantum key distribution via free-space, we take $\lambda_0=750\,{\rm nm}$, for which the photon is detected with the highest efficiency.[25]

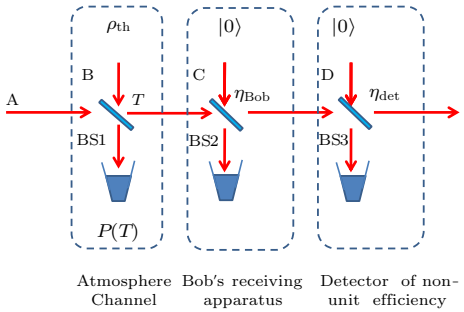

Fig. 2. (Color online) Simulation of the lossy channel with three beam splitters, $\rho_{\rm th}$. The transmittance coefficients of $\rm BS_1$, $\rm BS_2$ and $\rm BS_3$ are T, $\eta_{\rm Bob}$ and $\eta_{\rm det}$, respectively. The transmittance T is not fixed while a random variable obeys the probability distribution $P(T)$.

In Fig. 3, we investigate the decoy state quantum key distribution for increasing the transmission distance. We assume that two telescopes with radius $a_1=a_2=0.20\,{\rm m}$ are applied, which means $W_0=a_1=0.20\,{\rm m}$. Moreover, we choose $\mu=0.15$, $\nu_1=0.05$, $\nu_2=0.02$ and the weak turbulence condition $C_n^2=10^{-16}\,{\rm m}^{-2/3}$. To show the enhancement given by the decoy state method clearly, we can numerically evaluate the secret key rates of the decoy and non-decoy methods in the simplest case $n_{\rm th}=0$. Figures 3(a) and 3(b) show the difference of $Y_1^{\rm atom}$ and $Y_1^{\rm L}$ and the difference of single photon error rate e_1 and the estimation $e_1^{\rm U}$. Numerical results show that the difference is extremely small, which means that the estimation is performed within high precision. Moreover, $Y_1>Y_1^{\rm L}$ and $e_1<e_1^{\rm U}$ strictly holds for all transmission distance L: 0–100 km. Figure 3(c) shows the average transmittance $\langle T\rangle=\int P(T)TdT$ for increasing distance L. Finally, the secret key rates of quantum key distribution with decoy and without decoy state are clearly shown in Fig. 3(d). The quantum key distribution with no decoy state has a negligible small key generation rate after $L=17\,{\rm km}$ quantum

state transmission whereas the decoy method could support acceptable key rates even at 100 km.

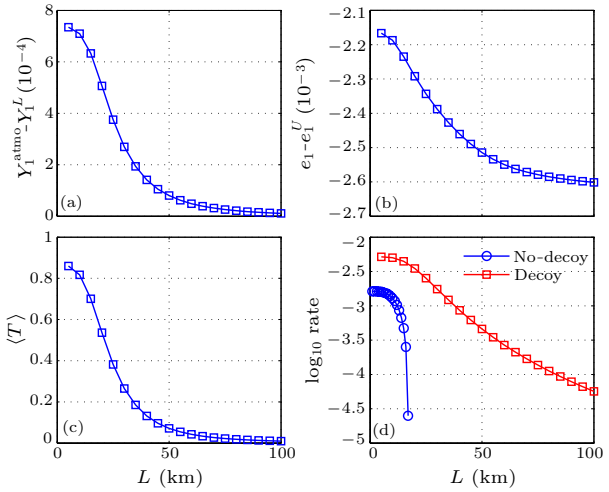

Fig. 3. (Color online) (a) Difference of $Y_1^{\rm atom}$ and $Y_1^{\rm L}$. (b) Difference of single photon error rate e_1 and the estimation $e_1^{\rm U}$. (c) Corresponding average transmittance of the atmosphere channel. (d) Secure key generation rate for key distribution with and without the decoy method. Other parameters are $\eta_{\rm Bob} = 0.45$, $\eta_{\rm det} = 0.80$, $f(E_\mu) = 1.10$, $C_n^2 = 10^{-16}\,{\rm m}^{-2/3}$ and $n_{\rm th} = 0$.

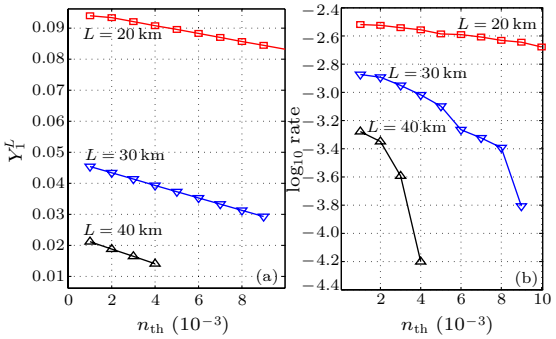

Fig. 4. (Color online) Effect of background noise (measured with average photon number $n_{\rm th}$) on the estimated single photon gain $Y_1^{\rm L}$ (a) and secret key rate given by the decoy state method (b). Other parameters ($\eta_{\rm Bob} = 0.45$, $\eta_{\rm det} = 0.80$, $f(E_\mu) = 1.10$, $C_n^2 = 10^{-16}\,{\rm m}^{-2/3}$) are identical to the ones in Fig. 3.

The effect of background noise can also be evaluated with non-zero $n_{\rm th}$. We again use the parameters in Fig. 3 and evaluate the single photon gain and secret key rate given by the decoy state method. We now change $n_{\rm th}$ from $n_{\rm th}$: 10^{-3}–10^{-2}. Actually, the values of $Y_1^{\rm L}$ and the key rate are not effected by the thermal noise of extreme level such that $n_{\rm th}$: 10^{-5}–10^{-3}. For each curve in Fig. 4, we fix the transmission distance $L = 20$, 30 and 40 km, respectively. For $L = 20$ km, we can still obtain the secret keys at a relatively high rate even at $n_{\rm th} = 10^{-2}$. However, such a phenomenon no longer exist at $L = 10$ km, for which the key rate drops exponentially at $n_{\rm th} \gtrsim 4\times10^{-3}$. This sheds more light on the importance of suppression of background noise in realistic implementation of quantum key distributions. To this point, the quantum communication in the evening seems to be one of the good choices for combating against background noise.[26]

In Fig. 5(a), we investigate the influence of atmosphere turbulence on the decoy state quantum key distribution. We consider the atmosphere channel of fixed length: $L = 20$ km. The secure key rate decreases monotonously as the structure constant C_n^2 increases. Figure 5(b) plots the dependence of average transmittance of the atmosphere channel on C_n^2. Numerical simulation shows that the key generation rate is dramatically decreased by atmosphere turbulence, which means that a crude estimation of atmosphere turbulence will spoil the security of decoy state quantum cryptography, which is assumably secure for a given level of signal and decoy state for ideal non-turbulence channels. Thus the characterization of atmosphere turbulence in realistic free-space based quantum key distributions would be one of the important procedures for carrying out realistic quantum key distribution tasks.

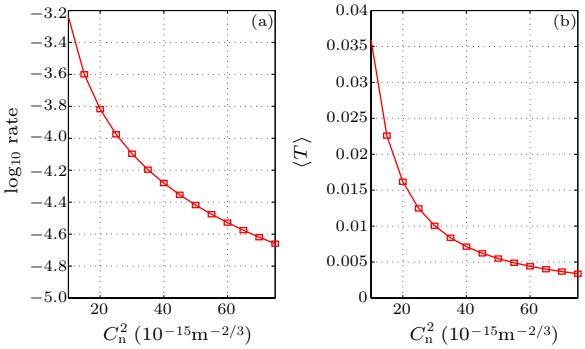

Fig. 5. (Color online) (a) Secure key rate of decoy state quantum key distribution for increasing atmosphere structure constant C_n^2 (in units of $10^{-15}\,{\rm m}^{-2/3}$). (b) Corresponding average transmittance of the atmosphere channel. Other parameters are $\eta_{\rm Bob} = 0.45$, $\eta_{\rm det} = 0.80$, $f(E_\mu) = 1.10$, $L = 20$ km and $n_{\rm th} = 0$.

Before concluding, it is quite interesting to compare the secure key rate generated via the fluctuating-lossy channel with the one in the standard attenuating channel with the transmission efficiency $\langle T\rangle = \int P(T)T dT$. Let us take the 15 km transmission as an example. We choose $\mu = 0.20$, $\nu_1 = 0.08$, $\nu_2 = 0.06$, $C_n^2 = 10^{-16}$, $n_{\rm th} = 0$ and we find that the secure key rates for the atmosphere channel and the standard attenuating channel follow $R_{\rm decoy}^{\rm atom} = 4.89\times10^{-3}$, $R_{\rm decoy}^{\rm standrad} = 4.88\times10^{-3}$, respectively. The difference is almost negligible since the key rate of QKD is dominated mostly by the single photon proportion, for which it follows directly that $Y_1^{\rm atom} = \int P(T)T\eta_{\rm Bob}\eta_{\rm det}dT = \langle T\rangle\eta_{\rm Bob}\eta_{\rm det}$. However, the difference may be enlarged if more thermal noise is introduced. For example, keeping all parameters fixed while $n_{\rm th} = 10^{-2}$, one obtains that $R_{\rm decoy}^{\rm atom} = 4.35\times10^{-3}$ and $R_{\rm decoy}^{\rm standrad} = 3.81\times10^{-3}$. The difference is due to the probability distribution of the transmission coefficient, which will influence the photon counts of the signal state and the decoy state in practical decoy state quantum key distribution protocol. We remark that recently a theory for reconstruction of PDTC has

been proposed[27] while relevant experimental verification is still being developed.

Atmosphere turbulence is an interesting while inevitable phenomenon in realistic free-space based quantum key distributions. In this study, we have chosen the beam-wandering model as an example and have investigated the possibility of the decoy state quantum key distribution in the presence of atmosphere turbulence. Our results represent a new trial of quantum key distribution in a fluctuating lossy channel, which becomes more and more important while open questions can be investigated along the same line. For example, due to the random turbulence and thus the consequent fluctuating channel efficiency, the distribution of bit error in the final sifted key will be different from the random distribution. This opens a new perspective to the Cascade-based[13] and LDPC-based key reconciliation[28] protocol for the key post-processing. Furthermore, we have analyzed the standard BB84 protocol implemented by the prepare-measurement method. The performance of recently-proposed device-independent quantum key distribution protocol[29] can also be analyzed by using the same method. Finally, the atmosphere turbulence is not the only channel with a fluctuating loss rate. In fact, even in the communication fiber of hundreds of kilometers, to keep the loss rate at a fixed level, is quite a difficult problem. It is believed that the corresponding models will be much closer to current experimental situations and more useful in free-space and fiber-based quantum key distribution protocols.

References

[1] Bennett C and Brassard G 1984 *IEEE International Conference on Computers, Systems and Signal Processing* p 175
[2] Bennett C et al 1992 *J. Cryptology* **5** 3
[3] Mo X F et al 2005 *Opt. Lett.* **30** 2632
[4] Liu Y et al 2010 *Opt. Express* **18** 8587
[5] Yin H L et al 2016 *Phys. Rev. Lett.* **117** 190501
[6] Dequal D et al 2016 *Phys. Rev.* A **93** 010301
[7] Rivest R L et al 1978 *Commun. ACM* **21** 120
[8] Gisin N et al 2002 *Rev. Mod. Phys.* **74** 145
[9] Wooters W K and Zurek W H 1982 *Nature* **299** 802
[10] Lodahl P et al 2015 *Rev. Mod. Phys.* **87** 347
[11] Lütkenhaus N 2000 *Phys. Rev.* A **61** 052304
[12] Gottesman D et al 2004 *Quantum Inf. Comput.* **4** 325
[13] Brassard G and Salvail L 1994 *Eurocrypt'93 Workshop Theory Application Cryptographic Tech. Adv. Cryptology.* **765** 410
[14] Wang X B 2005 *Phys. Rev. Lett.* **94** 230503
[15] Lo H K et al 2005 *Phys. Rev. Lett.* **94** 230504
[16] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901
[17] Fung C H F et al 2006 *Phys. Rev.* A **73** 012337
[18] Zhang S L et al 2009 *Chin. Sci. Bull.* **54** 1863
[19] Curty M et al 2009 *Phys. Rev.* A **79** 032335
[20] Vasylyev D Y et al 2012 *Phys. Rev. Lett.* **108** 220501
[21] Diament P and Teich M C 1970 *J. Opt. Soc. Am.* **60** 1489
[22] Peřina J 1972 *Czech. J. Phys.* **22** 1075
[23] Peřina J et al 1973 *Phys. Rev.* A **7** 1732
[24] Ishimaru A 1978 *The Beam Wave Case and Remote Sensing* (New York: Springer-Verlag) p 129
[25] http://www.idquantique.com/photon-counting/photon-counting-modules/id120/
[26] Kurtsiefer C et al 2002 *Nature* **419** 450
[27] Semenov A A et al 2012 *Phys. Rev.* A **85** 013826
[28] Kasai K et al 2010 *Inf. Reconciliation For QKD Rate-compatible Non-binary LDPC Codes.* (Int. Symp. Inf. Theory Its Appl.) p 922
[29] Lo H K et al 2012 *Phys. Rev. Lett.* **108** 130503