Orbital-angular-momentum-encoded free-space measurement device independent quantum key distribution

Zhu Zhuo-Dan[1] Zhao Shang-Hong[1] Dong Chen[2*]

[1] School of Information and Navigation, Air Force Engineering University, Xi'an 710077, China

[2*] Information and Communication College, National University of Defense and Technology, Xi'an 710006, China

Atmospheric turbulence, which causes the forward scattering of transmitted beam, has an adverse effect on the performance of orbital-angular-momentum(OAM)-encoded free-space measurement device independent quantum key distribution(MDI-QKD). In this paper, we quantify the turbulent influence of scattering OAM states by the probability of receiving the initial OAM modes, in conditions of both kolmogorov and non-kolmogorov turbulence. More practically, the secure key rates of OAM-encoded (MDI-QKD) are obtained under various turbulent intensity. From the Simulation results, when the radial coordinate increases, the initial OAM states are gradually diverted to adjacent modes and finally tend to be randomly distributed. Meanwhile, OAM-encoded MDI-QKD has a slightly longer maximum transmission distance than that of the polarization-encoded MDI-QKD.

Keywords：measurement device independent quantum key distribution; orbital angular momentum; atmospheric turbulence

1. Introduction

Quantum key distribution(QKD)[1-6] allow two distant parts, Alice and Bob, to establish a private encryption key in the presence of an eavesdropper. However, since the practical devices often fail to reach the theoretical security assumption, there is a series of attacks exploiting security loopholes of QKD systems[7-10]. In order to close loopholes on detection, a novel scheme called measurement device independent quantum key distribution(MDI-QKD)[11] is proposed, whose security is inspired by the time-reversed EPR-based QKD protocol.

In theory, Ma et al[12-13] proposed MDI-QKD protocols with decoy states. In experiment, Ref[14] implemented the proof-of-principle demonstration of MDI-QKD. Tang[15] achieved

three-nodes networking and Pan[16] implemented a 404km MDI-QKD experiment. However, the transmission losses of fibre channels increase exponentially with distance. Sufficiently large key rates can only be obtained over metropolitan-scale networks where the range is within 100 km.

An approach fitted with the present level of technology is to use free space links, whose attenuation is much less significant than fibre. Ursin et al[17-18] implemented QKD demonstrations in terrestrial free space. Micius satellite[19] performed BB84 protocol between satellite and ground. In free space link especially unlink configuration, optical loss is essentially dominated by atmospheric turbulence. The refractive index fluctuation can lead to wavefront distortion and amplitude fluctuation of light beam[20-22]. Therefore, it's great important to study the influence of atmospheric turbulence on single photon state, furthermore, on MDI-QKD protocol.

Apart from the polarization-encoded experiments above, orbital angular momentum(OAM) is an alternative encoding scheme for free-space QKD. Ref.[23] implemented an OAM-encoded QKD experiment under simulative turbulent atmosphere. Ref.[24] proposed a free-space OAM-encoded MDI-QKD scheme as well. There are at least two benefits using OAM encoding: 1. OAM states are rotational invariant in the transmission direction and can remove the error rate caused by reference frame misalignment[24]; 2. Since OAM theoretically has infinite dimensional eigenstate, key rate can be significantly improved by exploiting high-dimensional coding.

In this paper, we analyze the influence of atmospheric turbulence on scrambling OAM states. In condition of both kolmogorov and non-kolmogorov turbulence, The probability of scattering transmitted OAM state to adjacent OAM mode is obtained. Furthermore, the key generation rate and the maximal transmisstion distance of the OAM-encoded MDI-QKD under turbulence are analyzed. The simulation results show that with the propagation of light beam, the turbulent effect on scrambling OAM mode continuously enhanced, thus the probability of receiving initial OAM state decreases. And the maximal transmission distance of OAM-encoded MDI-QKD scheme is about 10 km longer than that of polarization-encoded MDI-QKD.

2. OAM-encoded MDI-QKD under atmospheric turbulence.

The spatial distribution of the OAM lead to its sensibility to atmospheric turbulence. The random fluctuation of turbulent medium results in the forward scattering of transmitted beam.

Since the influence of forward scattering on OAM is much greater than that on the spin of photons, so the scheme using OAM coding can't ignore the effect of turbulence.

2.1 Influence of atmospheric turbulence on OAM

When light beams tramsmitting through atmospheric turbulence, the refractive index fluctuation causes the random phase fluctuation of the beam, thus scattering finite-dimensional OAM states to adjacent OAM modes. Detailedly speaking, when a Laguerre Gaussian beam carrying $l_0\hbar$ units of OAM travels through atmospheric turbulence, the receiver may measure a photon with an OAM of $l_1\hbar$ *with* $l_1 \neq l_0$, introducing bit errors in quantum key distribution system.

The probability of receiving different adjacent OAM states can be written as[25]

$$P(l_0+\Delta l)=\frac{1}{2\pi^2R^2}\int_0^R rdr\int_0^{2\pi}d\theta_1\int_0^{2\pi}e^{-1/2\left\langle|\phi(r,\theta_1)-\phi(r,\theta_2)|^2\right\rangle}e^{i\Delta l(\theta_1-\theta_2)}d\theta_2 \quad (1)$$

Where $\Delta l=l_1-l_0$, r and θ are the radial coordinates and the azimuthal coordinates respectively, R is the radius of receiver aperture, and the quantity $\left\langle[\phi(r,\theta_1)-\phi(r,\theta_2)]^2\right\rangle$ is phase structure function. It can be evaluated by means of the non-kolmogorov turbulence theory to give the expression

$$\left\langle|\phi(r,\theta_1)-\phi(r,\theta_2)|^2\right\rangle = c_1\left|\frac{r_1-r_2}{\rho_0}\right|^{\alpha-2} \quad (2)$$

$$c_1=2\left(\frac{8}{\alpha-2}\Gamma\left[\frac{2}{\alpha-2}\right]\right)^{\frac{\alpha-2}{2}} \quad (3)$$

In which

$$\rho_0=\left(\mathrm{A}(\alpha)\mathrm{B}(\alpha)/C_n^2k^2L\right)^{\frac{1}{\alpha-2}}$$

$$\mathrm{A}(\alpha)=\frac{\Gamma(\alpha-1)\cos\left(\frac{\alpha\pi}{2}\right)}{4\pi^2},\quad \mathrm{B}(\alpha)=-2^{4-\alpha}\pi^2\Gamma\left[\frac{2-\alpha}{2}\right]\Big/\left\{2\left[8/(\alpha-2)\Gamma\left(\frac{2}{\alpha-2}\right)\right]^{\frac{2}{\alpha-2}}\Gamma\left(\frac{\alpha}{2}\right)\right\} \quad (4)$$

Where α is the spectral index, ρ_0 is generalized atmospheric coherence length, C_n^2 is the refractive-index structure parameter, k is the wave number, and L is propagation distance. When Eqs.(2) and (3) are introduced into Eqs.(1), the probability becomes

$$P(l_0+\Delta l)=\frac{1}{\pi}\int_0^1\rho d\rho\int_0^{2\pi}\exp\left[-2^{\alpha-2}\left(\frac{8}{\alpha-2}\Gamma\left[\frac{2}{\alpha-2}\right]\right)^{\frac{\alpha-2}{2}}\left(\frac{r}{\rho_0}\right)^{\alpha-2}\left|\sin\frac{\Delta\theta}{2}\right|^{\alpha-2}\right]\cos(\Delta l\Delta\theta)d\Delta\theta \quad (5)$$

This probability doesn't rely on the initial OAM quantum number l_0 but the amount Δl.

In particular, when the spectral index $\alpha = 11/3$, the non-kolmogorov model degrade into kolmogorov model, whose phase structure function is

$$\left\langle \left|\phi(r_1)-\phi(r_2)\right|^2 \right\rangle_2 = 6.88\left|\frac{r_1-r_2}{r_0}\right|^{5/3} \tag{6}$$

Correspondingly, the probability of receiving different adjacent OAM modes is

$$P(l_0+\Delta l)=\frac{1}{\pi}\int_0^1 \rho d\rho \int_0^{2\pi} \exp\left[-6.88\times 3^{\frac{2}{3}}\left(\frac{r}{r_0}\sin\frac{\Delta\theta}{2}\right)^{5/3}\right]\cos(\Delta l\Delta\theta)d\Delta\theta \tag{7}$$

On the other hand, $\Theta(r,\Delta l)$ is the scattering coefficient between azimuthal modes for optical power in an annulous of radius *r*.

$$\Theta(r,\Delta l)=\frac{1}{2\pi}\int_0^{2\pi} C_\phi(r,\Delta\theta)\exp(-i\Delta l\Delta\theta)d\Delta\theta \tag{8}$$

This coefficient depends on Δl but not l_1 as well. Here $C_\phi(r,\Delta\theta)=\exp[-1/2D_\phi(|2r\sin(\Delta\theta/2)|)]$ represents the rotational relation function and $D_\phi(|r_2-r_1|)=\left\langle|\phi(r_1)-\phi(r_2)|^2\right\rangle$ is the phase structure function. In the condition of kolmogorov turbulence, the scattering coefficient is

$$\Theta(r,\Delta l)=\frac{1}{2\pi}\int_0^{2\pi}\exp\left[-6.88\cdot 2^{\frac{2}{3}}\left(\frac{r}{r_0}\right)^{\frac{5}{3}}\left|\sin\frac{\Delta\theta}{2}\right|^{\frac{5}{3}}\right]\exp(-i\Delta l\Delta\theta)d\Delta\theta \tag{9}$$

2.2 Protocol and secure key rate

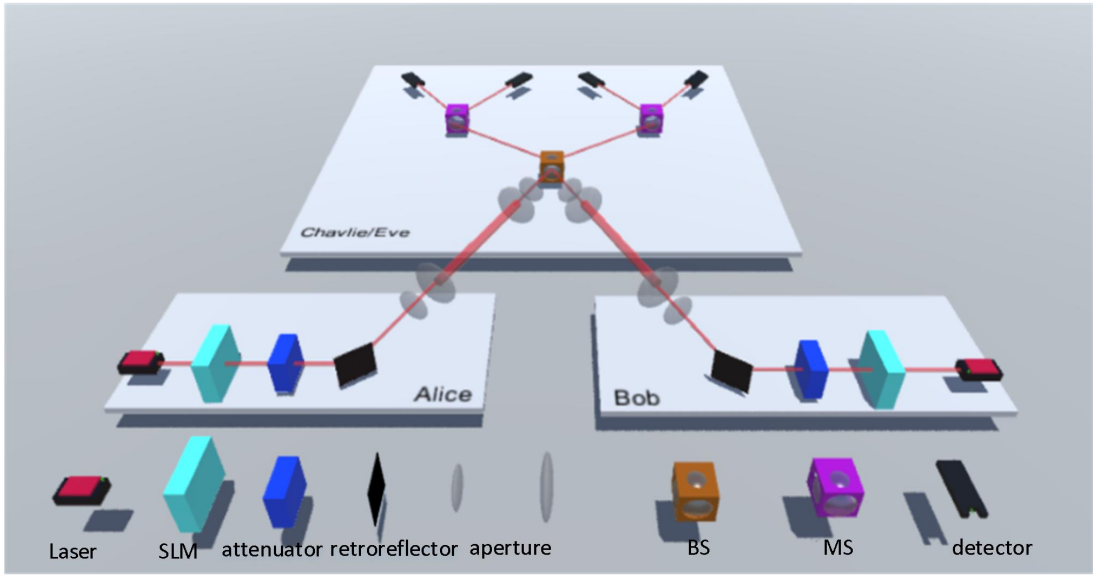

Fig. 1: Basic setup of OAM-encoded MDI-QKD.

OAM basis consist of $|-l\rangle$ and $|l\rangle$, SUP basis consist of $\frac{1}{\sqrt{2}}(|l\rangle+e^{in\pi}|-l\rangle)$ (n=0,1). Alice

and Bob choose independently one of two basis and modulate their quantum states by SLM. Then they attenuate weak coherent pulses to the single-photon level and get decoy states by an attenuator before entering free space link. In measurement parts, signal photons from Alice and Bob interfere at a 50:50 beam splitter (BS), projecting the input photons into Bell state. After comparing two parties' basis of each pulse, only the cases when they both choose OAM basis are used to generate secret-key bits.

We denotes η_0 as correct transmission probability, which shows the probability that the received OAM state is the same as transmitted one. And $\overline{\eta_0}$ is the corresponding transmission error probability. Thus

$$\eta_0 = \frac{e^{-\beta L}}{\pi}\int_0^1 \rho d\rho \int_0^{2\pi} \exp\left\{-2^{\alpha-2}\left[\frac{8}{\alpha-2}\Gamma\left(\frac{2}{\alpha-2}\right)\right]^{\frac{\alpha-2}{2}}\left(\frac{r}{\rho_0}\right)^{\alpha-2}\left|\sin\frac{\Delta\theta}{2}\right|^{\alpha-2}\right\} d\Delta\theta \quad (10)$$

$$\overline{\eta_0} = \frac{e^{-\beta L}}{\pi}\int_0^1 \rho d\rho \int_0^{2\pi} \exp\left\{-2^{\alpha-2}\left[\frac{8}{\alpha-2}\Gamma\left(\frac{2}{\alpha-2}\right)\right]^{\frac{\alpha-2}{2}}\left(\frac{r}{\rho_0}\right)^{\alpha-2}\left|\sin\frac{\Delta\theta}{2}\right|^{\alpha-2}\right\} \cos(2l\Delta\theta)\, d\Delta\theta \quad (11)$$

Where β is the link attenuation coefficient, $\rho = r/R$, and $\Gamma(\alpha)$ is the gamma function. Thus the total transmission rate is $\eta = \eta_0 + \overline{\eta_0}$, while the crosstalk probability $t = \dfrac{\overline{\eta_0}}{\eta}$.

The key rate is given by[12]

$$R = \mu\nu e^{-(\mu+\nu)} Y_{11}^{OAM}\left(1 - H\left(e_{11}^{SUP}\right)\right) - Q_{\mu\nu}^{OAM} f H\left(E_{\mu\nu}^{OAM}\right) \quad (12)$$

where f is error correction efficiency, $H_2(x)$ is binary Shannon entropy function. $Q_{\mu\nu}^{OAM}$ and $E_{\mu\nu}^{OAM}$ are total gain and error rate under OAM basis, which can be directly measured.

Here we assume both Alice and Bob can get infinite decoy states. Thus we have

$$Y_{11}^{OAM} = (1-P_d)^2\left[\frac{\eta_a\eta_b}{2} + (2\eta_a + 2\eta_b - 3\eta_a\eta_b)P_d + 4(1-\eta_a)(1-\eta_b)P_d^2\right] \quad (13)$$

where η_a（η_b） represents the total transmission of Alice（Bob）, P_d is the dark count rate of detector. $Y_{11}^{SUP} = Y_{11}^{OAM} = Y_E^{SUP} + Y_C^{SUP}$, where Y_E^{SUP} represents the yield of receiving wrong OAM state when two parties both use SUP basis, and Y_C^{SUP} represents the corresponding yield of receiving correct OAM state, which are both the functions of total transmissions of Alice and Bob.

Then the error rate of single photon can be written as

$$e_{11}^{SUP} = \frac{Y_E^{SUP} t_E + Y_C^{SUP} t_C}{Y_{11}^{SUP}} \tag{14}$$

Where t_E is the probability of receiving wrong state caused by misalignment of SUP basis or crosstalk, and t_C is the corresponding right probability.

3. Numerical Simulation

In this section, we numerically simulate the scattering coefficient and the probability of receiving adjacent OAM modes in condition of kolmogorov turbulence. More generally, the probabilities of receiving initial OAM state under different spectral indexes are indicated. Furthermore, we compare the secret key generation rate of OAM-encoded MDI-QKD scheme with that of polarization-encoded scheme.The numerical parameters are as follow.

Table 1 experimental parameters for Charlie/Eve[16]

e_d	P_d	f
1.5%	3×10^{-6}	1.16

Table 2 experimental parameters for Alice/Bob[24]

l	R (m)	λ (m)	β (dB/km)	C_n^2 ($m^{-2/3}$)
10	0.075	1.55×10^{-6}	0.6	10^{-15}

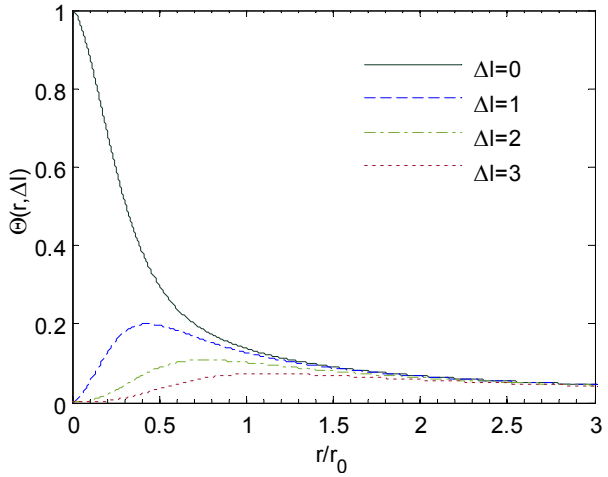

Fig.2 Scattering coefficients against the ratio of radial coordinates to the atmospheric coherence length.

By submitting $\Delta l = 0,1,2,3$ into Eqs.(9), Fig.2 shows scattering coefficient that the initial OAM states are scattered to different adjacent modes under kolmogorov turbulence. Here Δl represents the difference of OAM units before and after scattering.

r_0 is related to the spatial coherence length of the wavefront distortion. At the beginning of transmission, radial coordinates r is much smaller than r_0, and the phase distortion caused by atmospheric turbulence is slight, thus three scattering coefficients ($\Delta l = 1,2,3$) of initial OAM state are correspondingly small. As radial coordinates r increases, the cross-sectional area of beam gradually becomes wider, the range in which turbulence impact on beam increase as well, which result in the fast growth of three scattering coefficients. With radial coordinates's further growth, the initial OAM states tend to be scattered to infinite OAM states, the scattering coefficients reduce slowly.

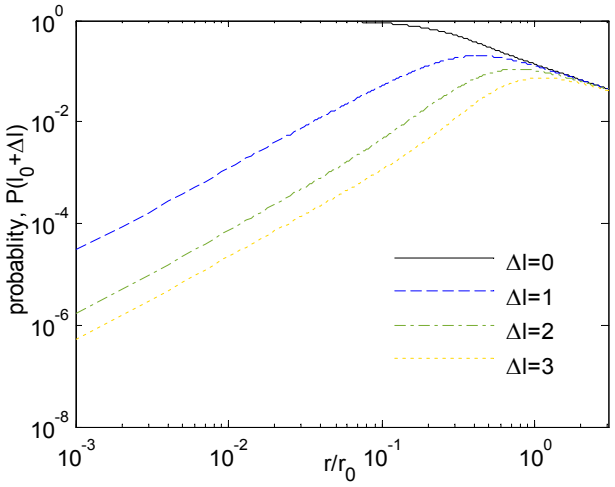

Fig.3 Probability of receiving adjacent modes versus the ratio of radial coordinates to the atmospheric coherence length.

Fig.3 shows that the phase aberration of the beam caused by turbulence is related to the radial coordinates r as well. At first, the probabilities of receiving adjacent modes ($\Delta l = 1,2,3$) increase with the growth of r, thus relatively reduce the probability of receiving the initial OAM states ($\Delta l = 0$). Then the probabilities of receiving adjacent modes decrease when r is comparable to r_0 and eventually OAM states tend to distribute randomly, which is in accordance with the conclusion of Fig.2.

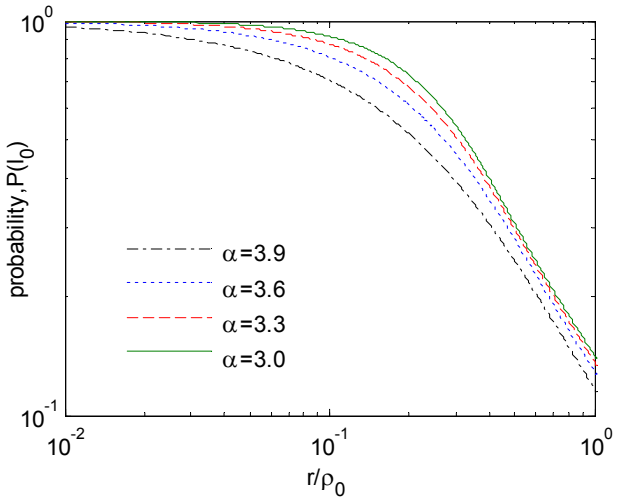

Fig.4 Probability of receiving original OAM states against the ratio of radial coordinates to the generalized atmospheric coherence length.

More generally, the influence of non-kolmogorov turbulence on the propagation of OAM states is analyzed. By submitting $\Delta l = 0$ into Eqs.(5), we can get the probability of receiving initial OAM states against the ratio of radial coordinates to the generalized atmospheric coherence length. From Fig.4, when spectral index α is fixed, the probability of receiving original OAM states decrease as the ratio r/ρ_0 increase. This is because since α is fixed, the higher r/ρ_0 corresponds to the bigger refractive index structure parameter and the stronger turbulence intensity, thus the OAM states are more scramble. Meanwhile, for every fixed ratio r/ρ_0, when spectral index increase, OAM states are more stable against atmospheric turbulence and the probability of receiving initial OAM states increase as well.

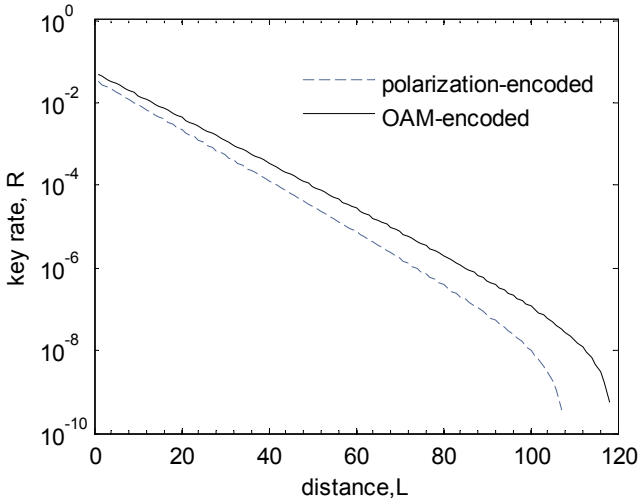

Fig.5 key rate versus transmission distance of different coding scheme.

Fig.5 shows the relationship between key rate and transmission distance of different coding

schemes. With the same simulation parameters, the maximal transmission distance of OAM-encoded MDI-QKD scheme is about 10km longer than that of polarization-encoded scheme. This is because the former scheme uses rotational invariant OAM basis , which reduces the single photon bit error rate caused by the misalignment of basis, and thus has a longer transmission distance.

4. Conclusion

In summary, We have analyzed OAM-encocded measurement device independent quantum key distribution under kolmogorov and non-kolmogorov turbulence. The turbulent effect on scattering OAM states is quantified by the scattering coefficient and the probability of receiving initial OAM modes. In condition of practical refractive-index structure parameters, secure key rates of OAM-encoded MDI-QKD are obtained. Simulation results indicate that the maximal transmission distance of OAM-encoded MDI-QKD is slightly longer than polarization-encoded MDI-QKD. And the secure key rate of OAM-encoded scheme decreases obviously as the intensity of the atmospheric turbulence increase. These results should prove useful in the design of practical free-space quantum key distribution systems.

References

[1] Lo H K, Lütkenhaus N. Quantum cryptography: from theory to practice[J]. Physics, 2007.

[2] Shor P W, Preskill J. Simple proof of security of the BB84 quantum key distribution protocol[J]. Physical Review Letters, 2000, 85: 441-444.

[3] Mayers D. Unconditional security in quantum cryptography[M]. ACM, 2001.

[4] Gottesman D, Lo H K, Lütkenhaus N, et al. Security of quantum key distribution with imperfect devices[C]// Information Theory, 2004. ISIT 2004. Proceedings. International Symposium on. IEEE, 2005:136.

[5] Gottesman D, Lo H K, Lutkenhaus N, et al. Security of quantum key distribution with imperfect devices[J]. Quantum Information & Computation, 2004, 4(5):325-360.

[6] Takesue H, Nam S W, Zhang Q, et al. Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors[J]. Nature Photonics, 2007, 1(17):5078-5081.

[7] Braunstein S L, Pirandola S. Measurement device independent quantum key distribution[J].

Physical Review Letters, 2012, 108(13):4089-4091.

[8] Brassard G, Lutkenhaus N, Mor T, et al. Limitations on practical quantum cryptography[J]. Physical Review Letters, 2000, 85(6):1330.

[9] Yuan Z L. Avoiding the blinding attack in QKD[J]. Nature Photonics, 2010, 4(4):800-801.

[10] Zhao Y, Fung C H F, Qi B, et al. Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems[C]// 2009 APS March Meeting. American Physical Society, 2009:4702-4705.

[11] Lo H K, Curty M, Qi B. Measurement-device-independent quantum key distribution[J]. Physical Review Letters, 2012, 108(13):130503.

[12] Ma X F, Fung C H F, Razavi M. Statistical fluctuation analysis for measurement-device-independent quantum key distribution[J]. Physical Review A, 2012, 86(5):052305.

[13] Sun S H, Gao M, Li C Y, et al. Practical decoy-state measurement-device-independent quantum key distribution[J]. Physical Review A, 2013, 87(5): 052329.

[14] Zhang Y C, Li Z Y, Yu S, et al. Continuous-variable measurement-device-independent quantum key distribution using squeezed states[J]. Physical Review A, 2014, 90(5):052325.

[15] Tang Y L, Yin H L, Chen S J, et al. Measurement-device-independent quantum key distribution over 200 km[J]. Physical Review Letters, 2014, 113(19):190501.

[16] Yin H L, Chen T Y, Yu Z W, et al. Measurement-Device-Independent Quantum Key Distribution Over a 404 km Optical Fiber[J]. Physical Review Letters, 2016, 117(19):190501.

[17] Schmitt-Manderbach T, Weier H, Fürst M, et al. Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km[J]. Physical Review Letters, 2007, 98(1):010504.

[18] Yin J, Ren J G, Lu H, et al. Quantum teleportation and entanglement distribution over 100-kilometre free-space channels[J]. Nature, 2012, 488(7410):185.

[19] Liao S K, Cai W Q, Liu W Y, et al. Satellite-to-ground quantum key distribution[J]. Nature, 2017, 549:7670.

[20] Bedington R, Arrazola J M, Ling A. Progress in satellite quantum key distribution[J]. Nature,2017, 3:30.

[21] Capraro I, Tomaello A, Dall'Arche A, et al. Impact of turbulence in long range quantum and classical communications[J]. Physical Review Letters, 2012, 109(20):200502.

[22] Vallone G, Marangon D G, Canale M, et al. Adaptive real time selection for quantum key distribution in lossy and turbulent free-space channels[J]. Physical Review A, 2015, 91(4):6206-6207.

[23] Goyal S, Ibrahim A H, Roux F S, et al. Experimental orbital angular momentum based quantum key distribution through turbulence[J]. arXiv ID: 1412.0788.

[24] Wang L, Zhao S M, Gong L Y, et al. Free-space measurement-device-independent quantum-key-distribution protocol using decoy states with orbital angular momentum[J]. Chinese Physics B, 2015, 24(12):238-245.

[25] Tyler G A, Boyd R W. Influence of atmospheric turbulence on the propagation of quantum states of light carrying orbital angular momentum[J]. Optics Letters, 2009, 34(2):142-4.