

Security analysis of satellite-to-ground reference-frame-independent quantum key distribution with beam wandering

Chun Zhou(周淳), Yan-Mei Zhao(赵燕美), Xiao-Liang Yang(杨晓亮), Yi-Fei Lu(陆宜飞), Yu Zhou(周雨), Xiao-Lei Jiang(姜晓磊), Hai-Tao Wang(汪海涛), Yang Wang(汪洋), Jia-Ji Li(李家骥), Mu-Sheng Jiang(江木生), Xiang Wang(汪翔), Hai-Long Zhang(张海龙), Hong-Wei Li(李宏伟), and Wan-Su Bao(鲍皖苏)

Citation: Chin. Phys. B, 2024, 33 (**8**): 080306. DOI: 10.1088/1674-1056/ad51f6
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

Improvement and security analysis of multi-ring discrete modulation continuous variable quantum secret sharing scheme

Huan-Yao Jiang(姜欢窈), Min Nie(聂敏), Guang Yang(杨光), Ai-Jing Sun(孙爱晶), Mei-Ling Zhang(张美玲), and Chang-Xing Pei(裴昌幸)
Chin. Phys. B, 2024, 33 (**7**): 070303. DOI: 10.1088/1674-1056/ad3b81

General multi-attack detection for continuous-variable quantum key distribution with local local oscillator

Zhuo Kang(康茁), Wei-Qi Liu(刘维琪), Jin Qi(齐锦), and Chen He(贺晨)
Chin. Phys. B, 2024, 33 (**5**): 050308. DOI: 10.1088/1674-1056/ad2bf2

A new quantum key distribution resource allocation and routing optimization scheme

Lin Bi(毕琳), Xiaotong Yuan(袁晓同), Weijie Wu(吴炜杰), and Shengxi Lin(林升熙)
Chin. Phys. B, 2024, 33 (**3**): 030309. DOI: 10.1088/1674-1056/ad2503

Improved decoy-state quantum key distribution with uncharacterized heralded single-photon sources

Le-Chen Xu(徐乐辰), Chun-Hui Zhang(张春辉), Xing-Yu Zhou(周星宇), and Qin Wang(王琴)
Chin. Phys. B, 2024, 33 (**2**): 020313. DOI: 10.1088/1674-1056/ad062a

Improved statistical fluctuation analysis for two decoy-states phase-matching quantum key distribution

Jiang-Ping Zhou(周江平), Yuan-Yuan Zhou(周媛媛), Xue-Jun Zhou(周学军), and Xuan Bao(暴轩)
Chin. Phys. B, 2023, 32 (**8**): 080306. DOI: 10.1088/1674-1056/acbdea

---

Security analysis of satellite-to-ground reference-frame-independent quantum key distribution with beam wandering

Chun Zhou(周淳)[1,2], Yan-Mei Zhao(赵燕美)[1,2,†], Xiao-Liang Yang(杨晓亮)[1,2], Yi-Fei Lu(陆宜飞)[1,2], Yu Zhou(周雨)[1,2], Xiao-Lei Jiang(姜晓磊)[1,2], Hai-Tao Wang(汪海涛)[1,2], Yang Wang(汪洋)[1,2], Jia-Ji Li(李家骥)[1,2], Mu-Sheng Jiang(江木生)[1,2], Xiang Wang(汪翔)[1,2], Hai-Long Zhang(张海龙)[1,2], Hong-Wei Li(李宏伟)[1,2], and Wan-Su Bao(鲍皖苏)[1,2,‡]

[1] *Henan Key Laboratory of Quantum Information and Cryptography, SSF IEU, Zhengzhou* 450001, *China*
[2] *Synergetic Innovation Centre of Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei* 230026, *China*

(Received 17 April 2024; revised manuscript received 29 May 2024; accepted manuscript online 30 May 2024)

The reference-frame-independent (RFI) quantum key distribution (QKD) is suitable for satellite-based links by removing the active alignment on the reference frames. However, how the beam wandering influences the performance of RFI-QKD remains a pending issue in satellite-to-ground links. In this paper, based on the mathematical model for characterizing beam wandering, we present the security analysis for satellite-to-ground RFI-QKD and analytically derive formulas for calculating the secret key rate with beam wandering. Our simulation results show that the performance of RFI-QKD is better than the Bennett–Brassard 1984 (BB84) QKD with beam wandering in asymptotic case. Furthermore, the degree of influences of beam wandering is specifically presented for satellite-to-ground RFI-QKD when statistical fluctuations are taken into account. Our work can provide theoretical support for the realization of RFI-QKD using satellite-to-ground links and have implications for the construction of large-scale satellite-based quantum networks.

Keywords: quantum key distribution, satellite-to-ground, beam wandering

PACS: 03.67.Dd, 03.67.Hk, 03.67.–a **DOI:** 10.1088/1674-1056/ad51f6

1. Introduction

Quantum key distribution (QKD)[1,2] is currently one of the most promising quantum technologies to achieve widespread practical application. However, the key rate of fiber-based QKD decreases exponentially[3,4] with the increase of distance. There are three ways to overcome this issue. One method is to promote the capability of quantum apparatus[5,6] to improve the performance of protocol[7–10] for extending the transmission distance of QKD system. Typically, the transmission distance has been achieved a vital breakthrough of 1000 km by conducting twin-field variant protocol.[5] The other method is to use quantum repeaters[11] that combine entanglement swapping,[12] entanglement purification,[13] and quantum memories.[14] Despite these laboratory technologies have been made progress[15–17] but they are still far from being applicable in practical long distance quantum communication. Another method is to develop satellite-based QKD based on space platform,[18] as the effective atmospheric thickness is only about 10 km.[19] Satellite-based QKD offers better flexibility than fiber-based QKD, allowing two parties to share secure keys in anywhere on the earth. Therefore, satellite-to-ground QKD provides crucial solution for achieving long-distance and large-scale global quantum communication networks.[20–24]

Since Micius's successful launch in 2016, series of key technologies for realizing satellite-to-ground QKD have been made great breakthroughs. All the experiments including these based on Bennett–Brassard 1984 (BB84) protocol[19,23,25] and those based on Bennett–Brassard–Mermin 1992 (BBM92) protocol[26,27] have been successfully demonstrated. In 2022, Micius satellite had achieved a new record of quantum state transmission on the earth's surface, covering a distance of 1200 km.[28] But entanglement-based QKD for space applications is facing many challenges.[29] Besides, existing experimental schemes require intermittent calibration of the reference frames during the satellite-to-ground communication process. In other words, communication parties need to keep the reference frames coincident from the beginning to end. Thus additional costs, such as communication resources and calibration modules, are required to guarantee the reliable operation of QKD system. Apparently, these would increase the complexity and difficulty of QKD experiments based on satellite-to-ground links. Fortunately, the reference-frame-independent QKD (RFI-QKD) proposed by Laing *et al.*[30] offers an alternative approach without calibrating, which enables two parties to negotiate secure keys regardless of the reference frames misalignment.

The RFI-QKD allows Alice and Bob to maintain consistency in Z basis, while the X and Y bases are allowed to slowly vary over time. In 2013, Wabnig *et al.*[31] first experimentally

†Corresponding author. E-mail: zym@qiclab.cn
‡Corresponding author. E-mail: bws@qiclab.cn

© 2024 Chinese Physical Society and IOP Publishing Ltd

demonstrated the feasibility of RFI-QKD based on free-space links in principle. Furthermore, Chun *et al.*[32] showed an approximate practical validation of free-space RFI-QKD based on a handheld transmitter module. They also took realistic finite-length effect into consideration and achieved a secret key rate above 30 kbits/s over a free-space distance of 0.5 m. In 2020, Xue *et al.*[33] first analyzed the effect of diffraction-caused attenuation on RFI-QKD based on uplink and downlink free-space channel, and improved the performance[34] of RFI-QKD through a turbulent atmosphere with pre-selection technology.[35] Actually, the weather conditions[36–40] play a major role in the transmission efficiency of photons in free-space links. For example, the existence of turbulent eddies and scattering particles,[40,41] such as haze or fog, undoubtedly results in unpredictable fluctuations of losses suffered by the quantum signals' broadening, wandering, and deformation[42–47] during the propagation along an atmospheric link. Therefore, it is of vital importance to study the effect of atmospheric properties on the performance of satellite-to-ground RFI-QKD. As beam broadening is easy to be characterized, the major sticking point is to analytically describe the beam wandering. To overcome this problem, Vasylyev *et al.* proposed a rigorous and general mathematical model[46] for characterizing beam wandering and applied it to the security analysis of decoy-state BB84-QKD protocol.[48,49] Then, Liorni *et al.*[37] conducted this model to present a comprehensive research on beam effects for satellite-to-ground QKD. Based on this model, studies related to beam wandering have been extended to measurement-device-independent QKD protocol[50,51] and continuous-variable QKD protocol.[52–55] Latest, Klen and Semenov[56] introduced an empirical model for a wide range of parameters. However, the influence of beam wandering on RFI-QKD performance in satellite-to-ground links remains an open question.

This paper discusses how the beam wandering of actual atmospheric downlink influence the performance of satellite-to-ground RFI-QKD. The security bound with beam wandering parameter and misalignment parameter of the reference frames is analytically derived. Based on the Micius's experimental parameters, the effect of beam wandering on the performance of satellite-to-ground RFI-QKD are simulated both in the asymptotic and nonasymptotic cases. The results show that the RFI-QKD protocol in the asymptotic case performs better than the BB84-QKD protocol but has equally sensitive to beam wandering. When taking statistical fluctuations resulted from finite key effect into account, one can find that the secret key rate decreases with a certain degree when beam drift and the reference frames error are both present and decreases significantly. Therefore, better pointing devices should be used as much as possible in free-space quantum communication to avoid beam wandering so as to maintain the stability of the links.

2. Free-space RFI-QKD protocol with decoy-state

In this section, we describe the satellite-to-ground RFI-QKD protocol. The protocol uses one-decoy setting and phase-randomized laser pulse to guarantee its security in the state-preparation step. Considering the vacuum + weak decoy-state method, Alice randomly modulates states with the three intensities μ_1, μ_2, and μ_3 ($\mu_1 > \mu_2 > \mu_3 = 0$), which are named as the signal state, decoy sate and vacuum state, respectively. In RFI-QKD, the Z basis is naturally well aligned for Alice and Bob during the whole communication, while the X basis and Y basis may vary with unknown deviation angle β as follows: $Z_{\rm B} = Z_{\rm A}, X_{\rm B} = \cos\beta X_{\rm A} + \sin\beta Y_{\rm A}, Y_{\rm B} = \cos\beta Y_{\rm A} - \sin\beta X_{\rm A}$. The feature of RFI-QKD is that establishing an intermediate quantity C from X and Y bases to bound Eve's knowledge.

Preparation: Alice generates one random ternary string $U \in \{0,1,2\}^N$ and one binary string $V \in \{1,-1\}^N$ with length N to decide the choose of basis and the classical bit. Here 0, 1, and 2 represent the Z basis, X basis, and Y basis, respectively. We denote that $|0\rangle$ and $|1\rangle$ consist of the Z basis, $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$ consist of the X basis, $|i\rangle = (|0\rangle + \mathrm{i}\,|1\rangle)/\sqrt{2}$ and $|-i\rangle = (|0\rangle - \mathrm{i}\,|1\rangle)/\sqrt{2}$ consist of the Y basis. The 1 in binary string $V \in \{1,-1\}$ represents the $|0\rangle$ in Z basis, the $|+\rangle$ in X basis and the $|i\rangle$ in Y basis, the -1 represents the $|1\rangle$ in Z basis, $|-\rangle$ in X basis and $|-i\rangle$ in Y basis. In each round, Alice modulates the intensities from μ_1, μ_2, and μ_3 with probabilities p_{μ_1}, p_{μ_2}, and p_{μ_3}, respectively. Then, Alice assigns bit values chosen uniformly from $U \in \{0,1,2\}^N$ and $V \in \{1,-1\}^N$ to prepare the phase-randomized laser pulse, where the Z basis, X basis, and Y basis are chosen with equal probability. These pulses from satellite are sent to ground station via free-space channel.

Measurement and sifting: Bob randomly selects a basis from $\{X_{\rm B}, Y_{\rm B}, Z_{\rm B}\}$ to measure pulse received from Alice, and informs Alice of his measurement result that the detector only one click as valid event through a public channel. Alice and Bob then publicly compare their basis for each pulse via an authenticated classical channel. When they both use the Z basis and a successful measurement event is announced, this pulse is recorded as a raw key. While these measurement results under X and Y bases are used for estimating the possible information leakage.

Parameter estimation: Alice and Bob use decoy-state method to estimate the gain and quantum bit error rate of single photon pulses in different bases combinations. The raw key consists of the case where they both chose Z basis, the quantum bit error can be calculated as e^1_{ZZ}. To estimate Eve's

knowledge, the key point of the RFI-QKD is that establishing an intermediate quantity C related to the quantum bit error in the combination $\{X_AX_B, X_AY_B, Y_AX_B, Y_AY_B\}$. Specifically, the number of information leaks I_E is intricately linked to the quantum bit errors e^1_{ZZ} and intermediary quantity C.

Processing: An error correction algorithm is applied to the raw key to ensure the consistency of the keys of both parties. At last, based on the information that leaks to the Eve, the privacy amplification step compresses their keys to some extent for extracting the final secret key.

It should be noted that RFI-QKD is apparently different from BB84-QKD protocol, specifically when estimating the Eve's knowledge. In RFI-QKD protocol, assuming that one direction is well defined and other directions are allowed to change with fixed value. Actually, in the satellite-to-ground links, information encoded in circular polarization is very stable, but the linear polarizations may vary in time. The main reason is that the satellite may be rotating with respect to the ground station. Here, figure 1 shows the schematic diagram of implementing RFI-QKD in satellite-to-ground links with beam wandering where the Z basis is naturally well aligned, whereas the X and Y bases between Alice and Bob may vary with an unknown deviation β.

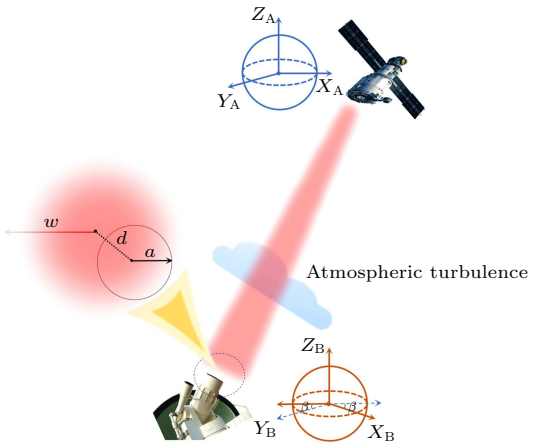


Fig. 1. The schematic diagram of implementing RFI-QKD in satellite-to-ground links with beam wandering. The radius of the receiving telescope is a. d is the long-term average distance between the center of receiving telescope and the center of beam light. w refers to the beam size after propagating a distance z.

3. Transmission efficiency of satellite-to-ground links

Here, we consider a ground station, a satellite in orbit at fixed altitudes $h = 500$ km, and variable zenith angles θ. The zenith is the angle between the direction of observation pointing at the satellite and the zenith point at the ground station. For the entire orbit of the satellite, the range of zenith angle values is from $-\pi/2$ to $\pi/2$, representing the forward horizontal position and backward one, respectively. Assuming $R_E \approx 6371$ km the approximate radius of the Earth,[57] based on geometric relations the slant distance between the ground and satellite can be written as $z(\theta) = \sqrt{h^2 + 2hR_E + R_E^2\cos^2\theta} - R_E\cos\theta$.

In satellite-to-ground quantum communication, transmission efficiency of quantum states carrying information through turbulence atmospheric is a critical factor for evaluating the performance of the whole protocol. The beam from satellite needs to travel the turbulent atmosphere that exhibits stochastic fluctuations caused by mixing of different temperature, pressure, and humidity. Besides, owning to the limited size of the receiving telescope and inevitable losses due to the quantum efficiency of the detector and other optical imperfections, the total transmission efficiency is often lower. In the following, as shown in Fig. 2, the attenuation caused by atmospheric extinction, beam broadening and wandering, is introduced.

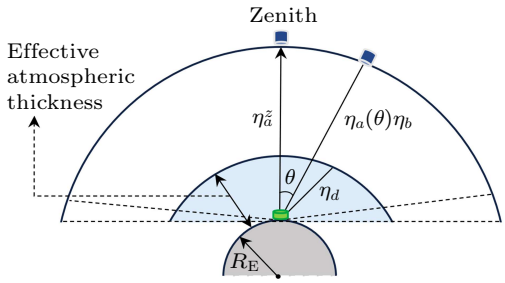


Fig. 2. The geometric distance and the transmission efficiency of satellite-to-ground. R_E is the approximate radius of the Earth, θ is the zenith angles. η_d is the attenuation introduced by the beam wandering.

First, atmospheric extinction is an important physical process that causes the loss of an optical beam during free-space propagation. This effect is described by the simple Beer–Lambert equation[57]

$$\eta_a = \exp\left(-\alpha\left(h\right)z\right), \tag{1}$$

where $\alpha(h) = \alpha_0 \exp\left(-h/\tilde{h}\right)$ is the extinction factor,[58] when $\tilde{h} = 6600$ m and $\lambda = 800$ nm, α_0 takes the approximate 5×10^{-6} m^{-1}, z represents the distance between satellite and ground station. When the satellite is at the zenith, the distance between the satellite and the ground station is equal to the altitude of the satellite's orbit. The authors in Ref. [57] defined the atmospheric extinction loss as

$$\begin{aligned} \eta_a^z &= \exp\left[-\int_0^h \mathrm{d}h'\alpha\left(h'\right)\right] \\ &= \exp\left[\alpha_0\tilde{h}\left(\mathrm{e}^{-h/\tilde{h}} - 1\right)\right] \\ &\geq \exp\left(-\alpha_0\tilde{h}\right) \approx 0.967. \end{aligned} \tag{2}$$

In the middle of the stratosphere, atmospheric density can be ignored after exceeding 30 km. Therefore, equation (2) takes into account the approximation at a height of 30 km. For zenith angles $\theta \neq 0$, in other words, the satellite is not directly above the ground station, the extinction loss can be expressed by using the analytical approximation method developed in Ref. [57]

$$\eta_a\left(z\right) \approx \left[\eta_a^z\right]^{\sec\theta}. \tag{3}$$

3.1. The maximum transmission efficiency

In this paper, we consider that quasi-monochromatic Gaussian beam is transmitted vertical from satellite to ground station, as depicted in Fig. 2. The beam propagating from satellite to receiver telescope needs to experience turbulence. The Rytov variance is employed to describe the strength of turbulence which is given by[57]

$$\sigma_{\mathrm{R}}^2 = 1.23 C_n^2 k^{7/6} L^{11/6}, \tag{4}$$

where k is wave number $k = 2\pi/\lambda$, λ is the wavelength, C_n^2 is the index-of-refraction structure constant, L is the distance of beam propagation. We approximate that the beam passes through the atmosphere with the same thickness in different zenith angles. According to Ref. [37], the value of C_n^2 inside the atmosphere is estimated by the integral average of function $C_n^2(h)$ in $[0,\infty]$ based on the H–V mode. Here h is the altitude. Thus, we assume C_n^2 as an average value. We equate the distance of beam propagation in the atmosphere to the effective thickness of the atmosphere, as the beam can be considered to propagate through a vacuum at other distances, free from atmospheric turbulence.

Because of the inevitable free-space diffraction and divergence angle, the spot size of the beam will broaden during propagation from satellite to receiver. When the distance is long, the broadening effect of the light beam through free space is determined by the propagation distance and divergence angle, the beam radius is given by

$$w = w_0 \left[1 + \left(\frac{\lambda z}{\pi w_0^2}\right)^2\right]^{1/2} \approx \frac{\lambda z}{\pi w_0} = \theta_{\mathrm{f}} z, \tag{5}$$

where w_0 is the initial spot size of beam, $\theta_{\mathrm{f}} = \lambda/(\pi w_0)$ is divergence angle (decided by the transmitter aperture, 5 μrad). Usually, the long-term beam radius w_{lt} and the short-term beam radius w_{st} approximately equal w for the satellite downlink.[57] The ratio (a/w) between the receiving aperture and the beam radius after transmission distance z varies with distance as in Fig. 3.

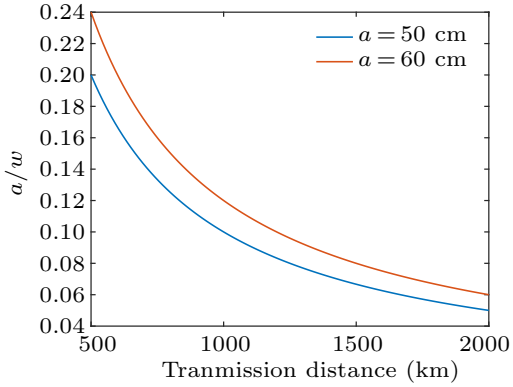


Fig. 3. The ratio of the radius of the receiving device a to the beam radius after transmission distance z varies with distance, a/w.

The quantum states of light in such channels are affected by fluctuating losses characterized by the probability distribution of transmittance (PDT). According to Ref. [56], it provides a more comprehensive study of the applicability range of the truncated log-normal distribution, the beam-wandering model, the elliptic-beam approximation, and the model based on the law of total probability. These model is shown to be strongly dependent on the ratio between the receiver aperture radius and the beam radius. The Beta distribution is inherently defined within the domain of $\eta \in [0,1]$ and in good agreement with numerical simulations for a wide range of channel parameters, especially for a/w less than 1. The PDT for the Beta-distribution model is shown

$$P(\eta) = \frac{1}{\mathrm{B}(a,b)} \eta^{a-1} (1-\eta)^{b-1}, \tag{6}$$

where $\mathrm{B}(a,b)$ is the Beta function. The parameters a and b are given by

$$a = a\left(\langle\eta\rangle, \langle\eta^2\rangle\right) = \frac{\langle\eta\rangle - \langle\eta^2\rangle}{\langle\eta^2\rangle - \langle\eta\rangle^2} \langle\eta\rangle, \tag{7}$$

$$b = b\left(\langle\eta\rangle, \langle\eta^2\rangle\right) = \frac{\langle\eta\rangle - \langle\eta^2\rangle}{\langle\eta^2\rangle - \langle\eta\rangle^2} (1 - \langle\eta\rangle). \tag{8}$$

The two moments $\langle\eta\rangle$ and $\langle\eta^2\rangle$ are described as the integral of the average beam intensity and intensity fluctuations over the receiving plane. By utilizing the parameters of existing Micius satellite, the probability distribution of transmission for different zenith angular can be calculated. According to classical atmospheric optics and the knowledge of optical radiation propagation, these two statistical quantities are depicted as field-correlation functions $\Gamma_2(\boldsymbol{r};L) = \langle I(\boldsymbol{r};L)\rangle$ and $\Gamma_4(\boldsymbol{r},\boldsymbol{r}';L) = \langle I(\boldsymbol{r};L) I(\boldsymbol{r}';L)\rangle$. Typically the beams from satellite are caused by aperture truncation of the light at the receiver. Then, the two moments of the channel transmission efficiency can be calculated as

$$\eta_b = \int_A \mathrm{d}^2\boldsymbol{r} I(\boldsymbol{r};L), \tag{9}$$

$$\langle\eta_b^2\rangle = \int_A \mathrm{d}^2\boldsymbol{r} \int_A \mathrm{d}^2\boldsymbol{r}' \Gamma_4(\boldsymbol{r},\boldsymbol{r}';L), \tag{10}$$

where A represents the area of the receiving aperture at distance $z = L$, $I(\boldsymbol{r};L)$ is the normalized Gaussian beam intensity concentrated on the plane of the receiving telescope $\boldsymbol{r} = [x,y]$. Simply, equation (9) can be approximated analytical expression of the form, expressed as[46]

$$\langle\eta_b\rangle = \int_A \mathrm{d}^2\boldsymbol{r} \Gamma_2(\boldsymbol{r};L) \approx 1 - \exp\left(-2\frac{a^2}{w^2}\right). \tag{11}$$

The scintillation index plays a critical role in the transmission of optical signal, its description remains one of the most challenging problem in free-space optics. Some works have been devoted to the scintillation index.[59,60] Generally,

fluctuations of the transmitted radiation are described by the aperture-averaged scintillation index

$$\sigma_\eta^2 = \frac{\langle \eta_b^2 \rangle - \langle \eta_b \rangle^2}{\langle \eta_b \rangle^2}. \tag{12}$$

The scintillation index is linked with the ratio of the beam radius to the receiver radius. When the aperture radius is reasonably larger than beam radius, the fluctuations of transmittance tending to zero. In the scenario considered in our paper, the beam radius from satellite is larger than the aperture radius. According to Ref. [61] for the satellite downlink, scintillation index is approximately considered to be the Rytov parameter for weak fluctuations ($\sigma_{\mathrm{R}}^2 < 1$), while scintillation index is rated to the Rytov parameter for weak-strong fluctuations, shown as

$$\sigma_\eta^2 \approx \begin{cases} \sigma_{\mathrm{R}}^2, & \sigma_{\mathrm{R}}^2 < 1, \\ \exp\left[\dfrac{0.49\sigma_{\mathrm{R}}^2}{\left(1+1.11\sigma_{\mathrm{R}}^{12/5}\right)^{7/6}} + \dfrac{0.51\sigma_{\mathrm{R}}^2}{\left(1+0.69\sigma_{\mathrm{R}}^{12/5}\right)^{5/6}}\right] - 1, & 1 < \sigma_{\mathrm{R}}^2 < \infty. \end{cases} \tag{13}$$

We can get $\langle \eta_b^2 \rangle$ through obtaining σ_η^2.

Considering the effects of atmospheric extinction, beam broadening, and inevitable intrinsic attenuation η_e (due to the detector efficiency and imperfections for other optical components), the maximum transmission efficiency can be expressed as

$$\langle \eta \rangle = \eta_e \langle \eta_b \rangle \eta_a(z). \tag{14}$$

Equation (14) calculates the maximum average transmission efficiency at a fixed distance. And the $\langle \eta^2 \rangle = \langle \eta_e^2 \eta_a^2(z) \eta_b^2 \rangle$ can be obtained. The the PDT for different zenith angles can be obtained based on the Beta distribution.

3.2. Beam wandering

It is difficult task to perfectly align between transmitter and receiver in practical scenario. We will consider the impact of beam wandering on transmission efficiency based on the law of total probability.[49] The beam wandering is an outcome of two independent factors, random errors in the pointing mechanism of the transmitter and the influence of atmospheric turbulence along the optical path. These two effects can be superimposed. According the analyses in Ref. [57], it has been computed by the scintillation index and the Rytov variance based on the Hufnagel–Valley model.[62,63]

Assuming that the beam center follows a normal distribution with variance σ^2 around a point at the distance d from the aperture center. Here, we extend this method to apply it to this scenario that when the long-term average wandering distance is fixed d caused by the combined effect atmospheric turbulence and pointing errors. The main idea based on the law of total probability is the separation of contributions from beam wandering and beam-spot distortions. Then we will calculate the $\langle \eta \rangle_d$ and $\langle \eta^2 \rangle_d$ based on the law of total probability. The conditional moment $\langle \eta \rangle_d$ can be considered as the transmittance through the aperture of this effective beam at the distance d from the aperture center, yields[49]

$$\langle \eta \rangle_d = \frac{\langle \eta \rangle}{\int_0^\infty \mathrm{d}\xi\, \xi\, \mathrm{e}^{-\xi^2/2} \mathrm{e}^{-[(\sigma/r_0)\xi]^s}} \exp\left[-\left(\frac{d}{r_0}\right)^s\right], \tag{15}$$

$$\langle \eta^2 \rangle_d = \frac{\langle \eta^2 \rangle}{\int_0^\infty \mathrm{d}\xi\, \xi\, \mathrm{e}^{-\xi^2/2} \mathrm{e}^{-2[(\sigma/r_0)\xi]^s}} \exp\left[-2\left(\frac{d}{r_0}\right)^s\right]. \tag{16}$$

The variance σ is introduced by the inaccuracy pointing of the transmitter as $\sigma_{\mathrm{p}}^2 = (\sigma_\theta z)^2$, where σ_θ refers to the source-deflection angle. Likewise, the variance introduced by atmospheric turbulence is denoted by $\sigma_{\mathrm{t}}^2 \approx 1.919 C_n^2 z^3 (2w_0)^{-1/3}$, where C_n^2 is the index-of-refraction structure constant. Generally, both variances should be added up, $\sigma^2 = \sigma_{\mathrm{p}}^2 + \sigma_{\mathrm{t}}^2$. We approximate that the beam passes through the atmosphere with the same thickness in different zenith angles. The average transmission efficiency will decrease with the average wandering distance d increase, which will increases the error rate and the instability of QKD system. In order to obtain parameters r_0 and s, two functions are introduced[46]

$$y_0(x) = \frac{1}{1 - \exp(-2x)\, \mathrm{I}_0(2x)}, \tag{17}$$

$$y_1(x) = \exp(-2x)\, \mathrm{I}_1(2x), \tag{18}$$

where I_n is the modified Bessel function of the first kind with order n, and other parameters are as follows:

$$s = \frac{4\eta_b^{\mathrm{f}} y_0\left(\eta_b^{\mathrm{f}}\right) y_1\left(\eta_b^{\mathrm{f}}\right)}{\ln\left[2\eta_b y_0\left(\eta_b^{\mathrm{f}}\right)\right]},$$

$$r_0 = a\left[\ln\left(2\eta_b y_0\left(\eta_b^{\mathrm{f}}\right)\right)\right]^{-1/s}, \tag{19}$$

where $\eta_b \simeq \eta_b^{\mathrm{f}} := 2a^2/w_{\mathrm{st}}^2$, the w_{st} is short-term beam radius, but we take $w_{\mathrm{st}} = w$, the reason is that we only consider satellite downlink and the detailed analyses were given by in Ref. [57]. The aperture-average scintillation index does not dependent on the deterministic losses. Then we can get $\langle \eta \rangle_d$ and $\langle \eta^2 \rangle_d$. The PDT for the Beta-distribution model is determined by two parameters a and b. Therefore, we can get PDT for beam wandering based on the Beta distribution.

4. Security analysis of RFI-QKD with beam wandering

The purpose of RFI-QKD[30] is to negotiate consistent and secure keys in situation that it is difficult to align the reference frames, such as satellite-to-ground links and the integrated photonic wave-guides. The satellite-to-ground RFI-QKD can be implemented on the existing devices, which can reduce experimental complexity compared with BB84-QKD protocol without calibration of the reference frames. However, when the emitted light beam passes through atmospheric turbulence, dominating disturbances due to beam broadening and wandering directly result in the reduction of transmission efficiency. Therefore, detailedly analyzing the performance of the satellite-to-ground RFI-QKD with beam wandering not only provides valuable insights into the behavior under practical scenarios but also serves as a theoretical foundation for future satellite-based experiments.

Considering the same parameters setting, it is necessary to compare the degree of tolerate beam wandering between BB84-QKD and RFI-QKD. Therefore, we present the asymptotic key rate formula of RFI-QKD[30]

$$R = Q^{1}_{ZZ}(1-I_{\mathrm{E}}) - fQ_{ZZ}H(E_{ZZ}), \tag{20}$$

where Q^{1}_{ZZ} is the single photon count rate in the ZZ basis combination, I_{E} is the number of information leaked to Eve. In the asymptotic case, we do not consider statistical fluctuations.

Due to the fact that infinite pulses cannot be achieved in practical QKD systems. So finite length analysis is needed in the real setting.[64] According the de Finetti theorem,[65] the finite length pulse key rate of RFI-QKD had been analyzed by Lana *et al.*,[66] which can against any coherent attacks. Here, we present the key rate of RFI-QKD based on the decoy state method[67–69] in the case of the nonasymptotic. So the finite length key rate formula is introduced[66]

$$\begin{aligned} R_N \geq \frac{1}{N}\Bigg[& \bar{s}^{1,\mathrm{L}}_{Z_{\mathrm{A}}Z_{\mathrm{B}}}\left(1-\left(1-\bar{e}^{1,\mathrm{U}}_{Z_{\mathrm{A}}Z_{\mathrm{B}}}\right)H\left(\frac{1+u}{2}\right)\right. \\ & \left.-\bar{e}^{1,\mathrm{U}}_{Z_{\mathrm{A}}Z_{\mathrm{B}}}H\left(\frac{1+v}{2}\right)\right) - f\bar{n}_{Z_{\mathrm{A}}Z_{\mathrm{B}}}H\left(\bar{E}_{Z_{\mathrm{A}}Z_{\mathrm{B}}}\right)\Bigg] \\ & -\frac{1}{N}\Bigg[\log_2\frac{2}{\varepsilon_{\mathrm{EC}}} - 2\log_2\frac{1}{\varepsilon_{\mathrm{PA}}} \\ & -7\sqrt{N_{ZZ}\log_2\frac{2}{\bar{\varepsilon}}} - 30\log_2(N+1)\Bigg], \end{aligned} \tag{21}$$

C now reads

$$\begin{aligned} \bar{C} = & \left(1-2\bar{e}^{1,\mathrm{U}}_{X_{\mathrm{A}}X_{\mathrm{B}}}\right)^2 + \left(1-2\bar{e}^{1,\mathrm{U}}_{X_{\mathrm{A}}Y_{\mathrm{B}}}\right)^2 + \left(1-2\bar{e}^{1,\mathrm{U}}_{Y_{\mathrm{A}}X_{\mathrm{B}}}\right)^2 \\ & + \left(1-2\bar{e}^{1,\mathrm{U}}_{Y_{\mathrm{A}}Y_{\mathrm{B}}}\right)^2, \end{aligned} \tag{22}$$

and

$$u = \min\left\{\frac{\sqrt{\bar{C}/2}}{1-\bar{e}^{1,\mathrm{U}}_{Z_{\mathrm{A}}Z_{\mathrm{B}}}}, 1\right\},$$

$$v = \frac{\sqrt{\bar{C}/2 - \left(1-e^{1,\mathrm{U}}_{Z_{\mathrm{A}}Z_{\mathrm{B}}}\right)u^2}}{\bar{e}^{1,\mathrm{U}}_{Z_{\mathrm{A}}Z_{\mathrm{B}}}}, \tag{23}$$

let

$$I_{\mathrm{E}} = \left(1-\bar{e}^{1,\mathrm{U}}_{Z_{\mathrm{A}}Z_{\mathrm{B}}}\right)H\left(\frac{1+u}{2}\right) - \bar{e}^{1,\mathrm{U}}_{Z_{\mathrm{A}}Z_{\mathrm{B}}}H\left(\frac{1+v}{2}\right), \tag{24}$$

where N is the total number of pulses, $H(x) = -\log_2 x - (1-x)\log_2(1-x)$ is the binary Shannon entropy function, $\bar{s}^{1,\mathrm{L}}_{Z_{\mathrm{A}}Z_{\mathrm{B}}}$ is the low bound of successful measurement cases when Alice sends single photon states in the $Z_{\mathrm{A}}Z_{\mathrm{B}}$ basis combination, $\bar{n}_{Z_{\mathrm{A}}Z_{\mathrm{B}}}$ refers the total number of successful counts for Alice and Bob in the Z basis, $\bar{e}^{1,\mathrm{U}}_{\gamma}$ represents the upper bound on the single-photon error rate in the events when the combination basis is γ, $\gamma \in \{Z_{\mathrm{A}}Z_{\mathrm{B}}, X_{\mathrm{A}}X_{\mathrm{B}}, X_{\mathrm{A}}Y_{\mathrm{B}}, Y_{\mathrm{A}}X_{\mathrm{B}}, Y_{\mathrm{A}}Y_{\mathrm{B}}\}$. According to the decoy-state method,[67–69] we can derive lower bound of single photon events $\bar{s}^{1,\mathrm{L}}_{\gamma}$, and the upper bound of corresponding QBER $\bar{e}^{1,\mathrm{U}}_{\gamma}$ of RFI-QKD

$$\begin{aligned} \bar{s}^{1,\mathrm{L}}_{Z_{\mathrm{A}}Z_{\mathrm{B}}} = & \frac{\mu_1\tau_1}{\mu_1\mu_2-\mu_2^2}\left[\frac{\mathrm{e}^{\mu_2}\bar{n}^{\mu_2,\mathrm{U}}_{Z_{\mathrm{A}}Z_{\mathrm{B}}}}{p_{\mu_2}} - \frac{\mu_1^2-\mu_2^2}{\mu_1^2}\frac{\mathrm{e}^{\mu_3}\bar{n}^{\mu_3,\mathrm{L}}_{Z_{\mathrm{A}}Z_{\mathrm{B}}}}{p_{\mu_3}}\right. \\ & \left. - \frac{\mu_2^2}{\mu_1^2}\frac{\mathrm{e}^{\mu_1}\bar{n}^{\mu_1,\mathrm{U}}_{Z_{\mathrm{A}}Z_{\mathrm{B}}}}{p_{\mu_1}}\right], \end{aligned} \tag{25}$$

$$\bar{e}^{1,\mathrm{U}}_{Z_{\mathrm{A}}Z_{\mathrm{B}}} = \frac{\tau_1}{\mu_2\bar{s}^{1,\mathrm{L}}_{Z_{\mathrm{A}}Z_{\mathrm{B}}}}\left(\frac{\mathrm{e}^{\mu_2}\bar{m}^{\mu_2,\mathrm{U}}_{Z_{\mathrm{A}}Z_{\mathrm{B}}}}{p_{\mu_2}} - \frac{\bar{m}^{\mu_3,\mathrm{L}}_{Z_{\mathrm{A}}Z_{\mathrm{B}}}}{p_{\mu_3}}\right), \tag{26}$$

where τ_1 is the total probability that Alice sends a single-photon state, $\bar{n}^{\chi}_{\gamma}$ and $\bar{m}^{\chi}_{\gamma}$ are the total counts and error counts when Alice chooses light intensity $\chi \in \{\mu_1, \mu_2, \mu_3\}$.

In the fiber-based QKD, transmission efficiency satisfies $\eta_{\mathrm{f}} = 10^{-\alpha L/10}$. So in a fixed experimental setup, the overall gain Q and QBER E remain constant when the transmission distance is certain, satisfying the following linear equations

$$Q^{\chi}_{\gamma}(\eta) = \sum_{n=0}^{\infty} p^{\chi}_{n} Y^{n}_{\gamma}, \tag{27}$$

$$Q^{\chi}_{\gamma}(\eta)E^{\chi}_{\gamma}(\eta) = \sum_{n=0}^{\infty} p^{\chi}_{n} Y^{n}_{\gamma} e^{n}_{\gamma}. \tag{28}$$

Here, we mainly focus on analyzing the performance of RFI-QKD in the satellite-to-ground links. When the zenith angle is fixed, the PDT is different with the instantaneous beam wandering distance. The overall gain and QBER under beam wandering need to be calculated as average values,

$$\bar{Q}(\theta) = \int_0^1 Q(\eta_i)P(\eta_i)\,\mathrm{d}\eta, \tag{29}$$

$$\bar{Q}(\theta)\bar{E}(\theta) = \int_0^1 Q(\eta_i)E(\eta_i)\,\mathrm{d}\eta, \tag{30}$$

where $\bar{Q}$ is the average of gain, $P(\eta_i)$ represents the probability distribution of the transmission efficiency under the beam

drift model. According to above equations, we can get the observed values count number of different bases combinations

$$\hat{n}_{\gamma}^{\chi} = N p_{\chi} \bar{Q}_{\gamma}^{\chi}. \tag{31}$$

Considering the limited number of pulses, we use improved Chernoff bound[70–72] to analyze statistical fluctuations, and the lower bound and the upper bound of expected values $\bar{n}_{\gamma}^{\chi}$ can be estimated using the observed values, satisfying the following expressions

$$\bar{n}_{\gamma}^{\chi,\mathrm{U}} = \frac{\hat{n}_{\gamma}^{\chi}}{1-\delta_{\mathrm{U}}}, \tag{32}$$

$$\bar{n}_{\gamma}^{\chi,\mathrm{L}} = \frac{\hat{n}_{\gamma}^{\chi}}{1+\delta_{\mathrm{L}}}, \tag{33}$$

with the failure probability at least $1-2\xi$, and the values δ_{U} and δ_{L} can be obtained by solving the following two equations:

$$\left[\frac{\mathrm{e}^{-\delta_{\mathrm{U}}}}{\left(1-\delta_{\mathrm{U}}\right)^{1-\delta_{\mathrm{U}}}}\right]^{X/(1-\delta_{\mathrm{U}})} = \xi, \tag{34}$$

$$\left[\frac{\mathrm{e}^{\delta_{\mathrm{L}}}}{\left(1+\delta_{\mathrm{L}}\right)^{1+\delta_{\mathrm{L}}}}\right]^{X/(1+\delta_{\mathrm{L}})} = \xi. \tag{35}$$

Similarly, the upper bound and lower bound of bit error number m_{γ}^{χ} can be obtained. By combining the equations provided earlier, we can get the lower bound of secret key rate of the decoy-state RFI-QKD. In the process of RFI-QKD over free-space channel, considering the fixed hardware parameters and statistical fluctuations, the average of the secret key rate of RFI-QKD over the PDT computed for different links lengths is given

$$\bar{R}(z) = \int_0^1 R(\eta)P(\eta)\,\mathrm{d}\eta = \sum_{i=1}^{N_b} R(\eta_i)\Delta\eta_i P(\eta_i), \tag{36}$$

$$\bar{R}_N(z) = \int_0^1 R_N(\eta)P(\eta)\,\mathrm{d}\eta = \sum_{i=1}^{N_b} R_N(\eta_i)\Delta\eta_i P(\eta_i), \tag{37}$$

when the zenith angle is fixed and the long-term beam wandering distance d is fixed, the transmission efficiency will show a probability distribution with the instantaneous beam wandering distance. Then we calculate the secure key rate of RFI-QKD at the particular zenith angle based on the probability distribution of transmission. It follows from the practical implications, $R(\eta)P(\eta) \geq 0$. The interval $[0,1]$ is inserted N_b points, $0 = \eta_0 < \eta_1 < \eta_2 < \cdots < \eta_{N_b-1} < \eta_{N_b} = 1$, diving the interval $[0,1]$ into N_b sub-intervals. The length of each sub-interval is, $\Delta\eta_1 = \eta_1 - \eta_0$, $\Delta\eta_2 = \eta_2 - \eta_1, \ldots$, $\Delta\eta_{N_b} = \eta_{N_b} - \eta_{N_b-1}$. When $\max\{\Delta\eta_1, \Delta\eta_2, \ldots, \Delta\eta_{N_b}\} \to 0$, the above integrals $\int_0^1 R(\eta)P(\eta)\,\mathrm{d}\eta$ can be approximated as $\sum_1^{N_b} \Delta\eta_i R(\eta_i)P(\eta_i)$.

5. Numerical simulation

With above analyses, we now numerically simulate the performance of RFI-QKD over the satellite-to-ground links with beam wandering. Firstly, we set the experimental parameters that we may use in our simulation. Then, we analyze and discuss our simulations results. The parameters are listed in Table 1.

Table 1. Simulation parameters.

Variable	Parameter	Simulation value
p_d	dark count rate	2×10^{-6}
e_d	intrinsic misalignment error	3.3%
C_n^2	atmospheric refractive index structure constant	10^{-14} m$^{-2/3}$
η_{e}	efficiency of experimental apparatuses	0.4
f	efficiency of error correction	1.16
λ	wavelength	800 nm
w_0	initial beam size	15 cm
a	receiving aperture size	60 cm
ξ	failure probability of statistical fluctuations analysis	10^{-10}

As shown in Fig. 4, we present the performance of infinite length pulse for RFI-QKD and BB84-QKD with or without beam wandering. We plot the max secret key rate which can be reached by the beam perfectly aligned between transmitter and receiver for RFI-QKD and BB84-QKD. When there is no beam wandering, the secret key rate (per pulse) of RFI-QKD is higher than BB84-QKD. The main reason is that the free-space links are complexity and have high intrinsic misalignment error. When this is not intrinsic misalignment error, the key rate of RFI-QKD and BB84-QKD is equivalent. With the increase of intrinsic misalignment error, the advantage of the RFI-QKD is more obvious. In a practical scenario, such alignment is very hard to realize even equipped with a multi-stage tracking device. So we consider a process of beam wandering with realistic scenario. As we can seen from Fig. 4, the secret key rate of RFI-QKD is slightly affected when the average wandering distance of between the center of the beam and the center of receiver is 0.2 m. When the beam radius from satellite to ground station will broaden exceeding the receiving telescope. Even if there has beam wandering, the process of distributing the quantum states can still continue at the expense of the secret key rate. Besides, we find that secret key rate is low even if the satellite being zenith, because the overall attenuation is considered to be greater than 20 dB.[23] We also can get that the RFI-QKD is outperformed BB84-QKD protocol regardless of the presence or absence of beam wandering when the intrinsic misalignment error is $e_d = 3.3\%$. The tolerable intrinsic misalignment error of RFI-QKD protocol is higher than BB84-QKD protocol.

Then, we analyze the influence of misalignment of reference frame β and the average distance of beam wandering d on decoy-state RFI-QKD in the asymptotic case. We simulate the effect beam wandering on secret key rate, i.e., $d = 0, 0.2$ m, 0.4 m with $\beta = 0, \pi/9$. As illustrated in Fig. 5, it is obvious

that the RFI-QKD can tolerate the deviation of the reference frames. When both reference frame error β and beam wandering d are present, the decoy RFI-QKD secure key rate will be severely affected. In practical scenario, due to the limitations of the technique, the tracking device start to work only when the zenith angle is greater than 10°.[23] Here, we only simulated the effect of the average beam wandering distance on the secure key rate when the zenith angle is less than 80°.

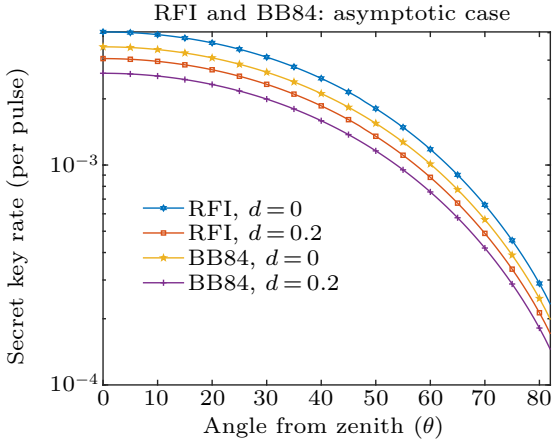


Fig. 4. Comparison between the BB84-QKD protocol and RFI-QKD protocol with and without beam wandering. The secret key rate (per pulse) in logarithmic scale *versus* zenith angle in the asymptotic case.

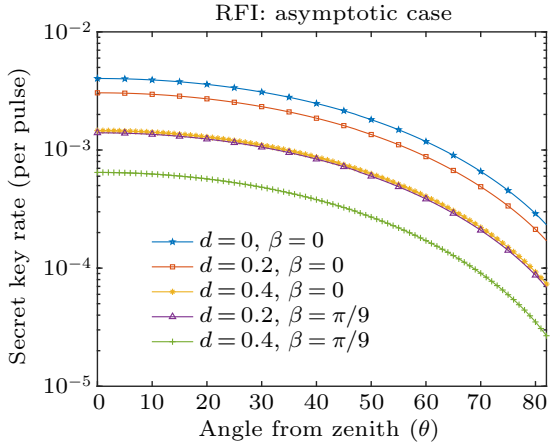


Fig. 5. Result of the RFI-QKD with and without reference deviation β in the asymptotic case. Different lines represent different parameter settings.

Due to the limited transit time of satellite, it is more practical to explore RFI-QKD with finite resources. As shown in Fig. 6, we mainly present the effect of beam wandering on the performance of decoy-state RFI-QKD for the finite pulse case. We numerically simulate the performance of RFI-QKD when the distance of beam wandering is set to be $d = 0.2$ m, 0.4 m, respectively. It is obvious that the drift distance has different influence on different total number of transmitted pulses N. Therefore, the lager of the total number of transmitted pulses, the smaller impact of beam wandering on the secure key rate. From an experimental point of view, the effect of beam wandering can be relaxed by increasing the total number of transmitted pulse. Due to the atmospheric is very complexity and more accurate results need to be got by conducting the experiment. Here, we just provide the theoretical reference.

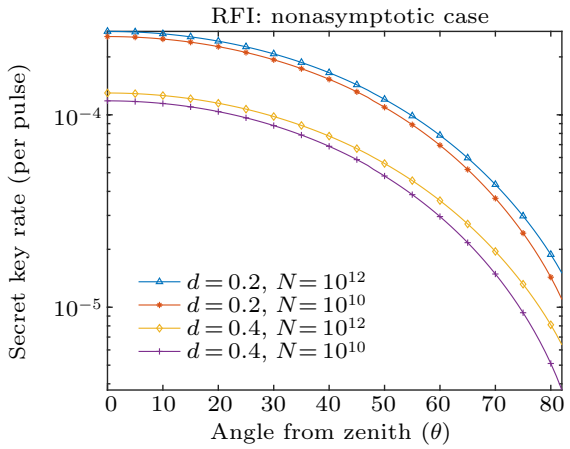


Fig. 6. The secret key rate (per pulse) in logarithmic scale *versus* zenith angle in the RFI-QKD for beam wandering ($d = 0.2$ m, 0.4 m) and different total numbers of transmitted pulses $N = 10^{12}$, 10^{10}.

As shown in Fig. 7, we simulate the effect of the reference frame misalignment β and beam wandering d on the performance satellite-to-ground RFI-QKD when $N = 10^{10}$. From the simulation result, we can see that the secret key rate decreases more significantly when beam drift and the reference frames error are both present. Besides, it has a detrimental effect on secret key rate when the distance of beam wandering exceeds 0.4 m. Therefore, satellite to ground QKD should be equipped with high-precision coarse tracking and fine tracking systems to maintain the stability of the transmission links.

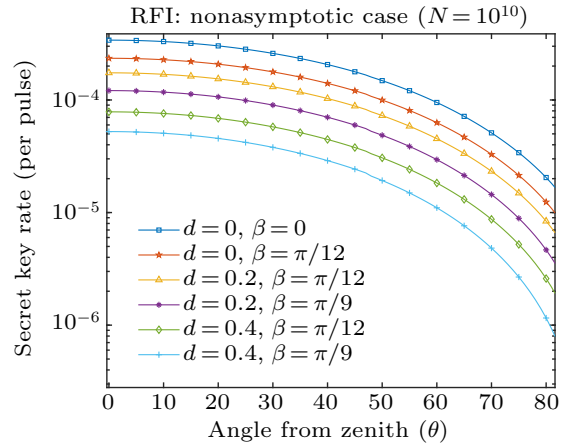


Fig. 7. The secret key rate (per pulse) in logarithmic scale *versus* zenith angle in the RFI-QKD for beam wandering ($d = 0$, 0.2 m, 0.4 m) and different deviations of reference frame $\beta = \pi/12, \pi/9$ for the total number of transmitted pulse $N = 10^{10}$.

In this paper, we simulated the degree of influences of beam wandering on the performance for the satellite-to-ground RFI-QKD protocol both in asymptotic and nonasymptotic cases. According to the simulation results, the RFI-QKD protocol in the asymptotic case performs better than the BB84-QKD protocol but has equally sensitive to beam wandering. Meanwhile, the satellite-to-ground RFI-QKD can tolerate beam wandering for the large data size while sensitive

to the small one when taking statistical fluctuations into account. This inspires us to keep the total number of transmitted pulse as longer as possible in practical RFI-QKD in satellite-to-ground links by increasing the frequency of light sources. Besides, when the beam wandering parameter and the reference frames deviation parameter are both existed, the secret key rate of RFI-QKD is dramatically decrease.

6. Conclusion

In conclusion, the atmospheric turbulence is complexity, randomness, and hard to predict, and we have merely theoretically analyzed the beam wandering. Specially, we have investigated the PDT of transmission efficiency for the satellite-to-ground links with and without beam wandering based on the Beta distribution model. When the transmission efficiency shows probability distribution, the formula for computing the protocol's key rate is derived. The simulation results show that as long as the beam is not completely deflected from the receiving telescope, then the secret key will be generated. Besides, we find that the bad effects of beam wandering can be relaxed by increasing the length of the pulses. Hence, the high-speed QKD system should be developed for the satellite-to-ground links. Indeed, during the whole process of the satellite-ground links communication, the transmission efficiency tends to be low and the QBER is relatively high. Therefore, one can resort to the advantage distillation technology introduced by Jiang *et al.*[73] to improve the secret key rate.

Actually, incorporating different atmospheric parameters, such as temperature, pressure, humidity, and wind speed as input parameters, and the distance of beam wandering as output parameter in this model is absent. In the future, beam wandering introduced by atmospheric turbulence can be compensated through building a more realistic model. In addition, accurate tracking devices should be used as much as possible in free-space quantum communication to avoid beam wandering and to maintain the stability of links. Based on our work, it can provide guidance for developing calibration and compensation techniques in the design of free-space QKD.

Acknowledgements

Project supported by the National Natural Science Foundation of China (Grant Nos. 61505261, 62101597, 61605248, and 61675235), the National Key Research and Development Program of China (Grant No. 2020YFA0309702), the China Postdoctoral Science Foundation (Grant No. 2021M691536), the Natural Science Foundation of Henan Province, China (Grant Nos. 202300410534 and 202300410532), and the Fund of the Anhui Initiative in Quantum Information Technologies.

References

[1] Bennett C H and Brassard G 2014 *Theor. Comput. Sci.* **560** 7
[2] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[3] Takeoka M, Guha S and Wilde M M 2014 *Nat. Commun.* **5** 5235
[4] Pirandola S, Laurenza R, Ottaviani C and Banchi L 2017 *Nat. Commun.* **8** 15043
[5] Liu Y, Zhang W J, Jiang C, Chen J P, Zhang C, *et al.* 2023 *Phys. Rev. Lett.* **130** 210801
[6] Wang S, Yin Z Q, He D Y, Chen W, Wang R Q, *et al.* 2022 *Nat. Photon.* **16** 154
[7] Lucamarini M, Yuan Z L, Dynes J F and Shields A J 2018 *Nature* **557** 400
[8] Ma X F, Zeng P and Zhou H Y 2018 *Phys. Rev. X* **8** 031043
[9] Wang X B, Yu Z W, Hu and X L 2018 *Phys. Rev. A* **98** 062323
[10] Xie Y M, Lu Y S, Weng C X, Cao X Y, Jia Z Y, *et al.* 2017 *PRX Quantum* **3** 020315
[11] Briegel H J, Dür W, Cirac J I and Zoller P 1998 *Phys. Rev. Lett.* **81** 5932
[12] Zukowski M, Zeilinger A, Horne M A and Ekert A K 1993 *Phys. Rev. Lett.* **71** 4287
[13] Bennett C H, Brassard G, Popescu S, Schumacher B, Smolin J A, *et al.* 1996 *Phys. Rev. Lett.* **76** 722
[14] Duan L M, Lukin M D, Cirac J L and Zoller P 2001 *Nature* **414** 413
[15] Pan J W, Bouwmeester D, Weinfurter H and Zeilinger A 1998 *Phys. Rev. Lett.* **80** 3891
[16] Pan J W, Gasparoni S, Ursin R, Weihs G and Zeilinger A 2003 *Nature* **423** 417
[17] Yang S J, Wang X J, Bao X H and Pan J W 2016 *Nat. Photon.* **10** 381
[18] Vallone G, Bacco D, Dequal D, Gaiarin S, Luceri V, *et al.* 2015 *Phys. Rev. Lett.* **115** 040502
[19] Liao S K, Cai W Q, Liu W Y, Zhang L, Li Y, *et al.* 2017 *Nature* **549** 43
[20] Kimble H J 2008 *Nature* **453** 1023
[21] Wehner S, Elkouss D and Hanson R 2018 *Science* **362** 9288
[22] Wang S, Chen W, Yin Z Q, Li H W, He D Y, *et al.* 2014 *Opt. Express* **22** 21739
[23] Chen Y A, Zhang Q, Chen T Y, Cai W Q, Liao S K, *et al.* 2021 *Nature* **589** 214
[24] Sidhu J S, Joshi S K, Gündoğan M, Brougham T, Lowndes D, *et al.* 2021 *IET Quantum Communication* **2** 182
[25] Li Y, Liao S K, Cao Y, Ren J G, Liu W Y, *et al.* 2022 *Optica* **9** 933
[26] Yin J, Li Y H, Liao S K, Yang M, Cao Y, *et al.* 2020 *Nature* **582** 501
[27] Yin J, Cao Y, Li Y H, Ren J G, Liao S K, *et al.* 2017 *Phys. Rev. Lett.* **119** 200501
[28] Li B, Cao Y, Li Y H, Cai W Q, Liu W Y, *et al.* 2022 *Phys. Rev. Lett.* **128** 170501
[29] Ecker S, Pseiner J, Piris J and Bohmann M 2023 *International Conference on Space Optics-ICSO* **12777** 925
[30] Laing A, Scarani V, Rarity J G and O'Brien J L 2010 *Phys. Rev. A* **82** 012304
[31] Wabnig J, Bitauld D, Li H W, Laing A, O'brien J L, *et al.* 2013 *New J. Phys.* **15** 073001
[32] Chun H, Choi I, Faulkner G, Clarke L and Barber B, *et al.* 2017 *Opt. Express* **25** 6784
[33] Xue Y, Shi L, Wei J H, Yu L L, Yu H C, *et al.* 2020 *Int. J. Theor. Phys.* **59** 3299
[34] Xue Y, Shi L, Chen W, Yin Z Q, Fan Yuan G J, *et al.* 2020 *Phys. Rev. A* **102** 062602
[35] Wang W Y, Xu F H and Lo H K 2018 *Phys. Rev. A* **97** 032337
[36] Vasylyev D, Semenov A A, Vogel W, Günthner K, Thurn A, *et al.* 2017 *Phys. Rev. A* **96** 043856
[37] Liorni C, Kampermann H and Bruß D 2019 *New J. Phys.* **21** 093055
[38] Chen H, Wang J P, Tang B Y, Li Z H, Liu B, *et al.* 2020 *Opt. Lett* **45** 3022
[39] Scriminich A, Foletto G, Picciariello F, Stanco A, Vallone G, *et al.* 2022 *Quantum Sci. Technol.* **7** 045029
[40] Lu Q H, Wang F X, Huang K, Wu X, Wang Z H, *et al.* 2022 *Phys. Rev. Appl.* **17** 034045
[41] Henniger H and Wilfert O 2010 *Radioengineering* **19** 2
[42] Zhu X M and Kahn J M 2002 *IEEE Trans. Commun.* **50** 1293
[43] Hulea M, Ghassemlooy Z, Rajbhandari S and Tang X 2014 *J. Light. Technol.* **32** 1323

[44] Milonni P W, Carter J H, Peterson C G and Hughes R J 2004 *J. Opt. B: Quantum Semiclassical Opt.* **6** S742
[45] Semenov A A and Vogel W 2009 *Phys. Rev. A* **80** 021802
[46] Vasylyev D Y, Semenov A A and Vogel W 2012 *Phys. Rev. Lett.* **108** 220501
[47] Vasylyev D, Semenov A A and Vogel W 2016 *Phys. Rev. Lett.* **117** 090501
[48] Vasylyev D, Vogel W and Moll F 2019 *Phys. Rev. A* **99** 053830
[49] Vasylyev D, Vogel W and Semenov A A 2018 *Phys. Rev. A* **97** 063852
[50] Liang W T and Jiao R Z 2020 *New J. Phys.* **22** 083074
[51] Dong Q, Huang G Q, Cui W and Jiao R Z 2021 *Quantum Sci. Technol.* **7** 015014
[52] Derkach I and Usenko V 2023 *International Conference on Space Optics-ICSO* **12777** pp. 1089–1103
[53] Hu H Y, Zhong H, Ye W and Guo Y 2022 *Commun. Theor. Phys.* **74** 125102
[54] Dequal D, Trigo V L, Roman R V, Vallone G, Villoresi P, *et al*. 2021 *NPJ Quantum Inf.* **7** 3
[55] Wang S Y, Huang P, Wang T and Zeng G H 2018 *New J. Phys.* **20** 083037
[56] Klen M and Semenov A A 2023 *Phys. Rev. A* **108** 033718
[57] Pirandola S 2021 *Phys. Rev. Res.* **3** 023130
[58] Bohren C F and Huffman D R 2008 *Absorption and scattering of light by small particles* (Chichester: John Wiley and Sons)
[59] Baskov R A and Chumak O O 2020 *J. Opt.* **22** 105603
[60] Baskov R 2022 *Phys. Rev. A* **105** 063713
[61] Andrews L C and Phillips R L 2005 *Laser Beam Propagation Through Random Media: Second Edition* (Bellingham: SPIE-International Society for Optical Engineering)
[62] Hufnagel R E and Stanley N R 1964 *JOSA* **54** 52
[63] Valley G C 1980 *Appl. Opt.* **19** 574
[64] Sidhu J S, Brougham T, McArthur D, Pousa, Roberto G and Oi Daniel K L 2022 *NPJ Quantum Inf.* **8** 18
[65] Christandl M, König R and Renner R 2009 *Phys. Rev. Lett.* **102** 020504
[66] Sheridan L, Le T P and Scarani V 2010 *New J. Phys.* **12** 123019
[67] Wang X B 2005 *Phys. Rev. Lett.* **94** 230503
[68] Lo H K, and Ma X F and Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[69] Ma X F, Qi B Zhao Y and Lo H K 2005 *Phys. Rev. A* **72** 012326
[70] Chernoff H 1952 *Ann. Math. Stat.* 493
[71] Curty M, Xu F H, Cui W, Lim C C W, Tamaki K, *et al*. 2014 *Nat. Commun.* **5** 3732
[72] Zhang Z, Zhao Q, Razavi M and Ma X F 2017 *Phys. Rev. A* **95** 012333
[73] Jiang X L, Wang Y, Li J J, Lu Y F, Hao C P, *et al*. 2023 *Opt. Express* **31** 9196