

Improving the performance of reference-frame-independent measurement-device-independent quantum key distribution in hybrid channels

Yan-Mei Zhao(赵燕美), Chun Zhou(周淳), Xiao-Lei Jiang(姜晓磊), Yi-Fei Lu(陆宜飞), Yu Zhou(周雨), Hai-Tao Wang(汪海涛), Yang Wang(汪洋), Jia-Ji Li(李家骥), Yan-Yang Zhou(周砚扬), Hong-Wei Li(李宏伟), and Wan-Su Bao(鲍皖苏)

Citation: Chin. Phys. B, 2025, 34 (**5**): 050302. DOI: 10.1088/1674-1056/adbee4
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

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

Asymmetric mode-pairing quantum key distribution with advantage distillation

Hai-Tao Wang(汪海涛), Chun Zhou(周淳), Yi-Fei Lu(陆宜飞), Chen-Peng Hao(郝辰鹏), Yan-Mei Zhao(赵燕美), Yan-Yang Zhou(周砚扬), Hong-Wei Li(李宏伟), and Wan-Su Bao(鲍皖苏)
Chin. Phys. B, 2025, 34 (**4**): 040305. DOI: 10.1088/1674-1056/adbb5c

Mask-coding-assisted continuous-variable quantum direct communication with orbital angular momentum multiplexing

Zhengwen Cao(曹正文), Yujie Wang(王禹杰), Geng Chai(柴庚), Xinlei Chen(陈欣蕾), and Yuan Lu(卢缘)
Chin. Phys. B, 2025, 34 (**2**): 020308. DOI: 10.1088/1674-1056/ad9ff7

Improved reference-frame-independent quantum key distribution with intensity fluctuations

Zi-Qi Chen(陈子骐), Hao-Bing Sun(孙昊冰), Ming-Shuo Sun(孙铭烁), and Qin Wang(王琴)
Chin. Phys. B, 2025, 34 (**2**): 020302. DOI: 10.1088/1674-1056/ad99cb

Effect of pseudo-random number on the security of quantum key distribution protocol

Xiao-Liang Yang(杨晓亮), Yu-Qing Li(李毓擎), and Hong-Wei Li(李宏伟)
Chin. Phys. B, 2025, 34 (**2**): 020301. DOI: 10.1088/1674-1056/ad99c9

Multi-protocol relay chaining for large-scale quantum key distribution networks

Yuan Cao(曹原), Xiaosong Yu(郁小松), Yongli Zhao(赵永利), Chunhui Zhang(张春辉), Xingyu Zhou(周星宇), Jie Zhang(张杰), and Qin Wang(王琴)
Chin. Phys. B, 2025, 34 (**1**): 010310. DOI: 10.1088/1674-1056/ad9018

SPECIAL TOPIC — Quantum communication and quantum network

Improving the performance of reference-frame-independent measurement-device-independent quantum key distribution in hybrid channels

Yan-Mei Zhao(赵燕美), Chun Zhou(周淳)†, Xiao-Lei Jiang(姜晓磊), Yi-Fei Lu(陆宜飞), Yu Zhou(周雨), Hai-Tao Wang(汪海涛), Yang Wang(汪洋), Jia-Ji Li(李家骥), Yan-Yang Zhou(周砚扬), Hong-Wei Li(李宏伟), and Wan-Su Bao(鲍皖苏)‡

Henan Key Laboratory of Quantum Information and Cryptography, SSF IEU, Zhengzhou 450001, *China*

(Received 9 January 2025; revised manuscript received 25 February 2025; accepted manuscript online 11 March 2025)

The robustness of reference-frame-independent measurement-device-independent quantum key distribution (RFI-MDI-QKD) against detection system vulnerabilities and its tolerance to reference frame drifts make it an ideal choice for hybrid channels. However, the impact of atmospheric turbulence on transmittance fluctuations remains a significant challenge for enhancing the performance of RFI-MDI-QKD. In this paper, we apply prefixed-threshold real-time selection and advantage distillation techniques to RFI-MDI-QKD in a hybrid channels scenario. Then, we analytically derive formulas for secret key rate in hybrid channels. Simulation results show that our modified scheme has apparent advances in both maximum tolerant loss and secure key rate compared to the fiber-only channel. Specifically, the result demonstrates that the maximum transmission distance can be improved by 15 km and 28 km when $N = 10^{12}$ and 10^{11}. Our work not only provides a more robust key distribution protocol but also establishes a solid theoretical foundation for enhancing the performance of RFI-MDI-QKD in hybrid channels.

Keywords: quantum key distribution, measurement-device-independent, hybrid channels

PACS: 03.67.Dd, 03.67.Hk, 03.67.–a

DOI: 10.1088/1674-1056/adbee4 **CSTR:** 32038.14.CPB.adbee4

1. Introduction

Quantum key distribution (QKD) based on the theory of quantum mechanics allows distant individuals to share keys. The ultimate goal of quantum communication is to establish a practical quantum network with real-time, secure coverage across various geographical scales from local-area to wide-area.[1–3] In general, the development of fiber-based QKD is technologically mature,[4–7] and satellite-to-ground QKD has been successfully demonstrated.[8–10] Meanwhile, a series of fruitful achievements have been made[11–16] in the field of QKD. In a future continental-scale quantum network, satellite, airplane, unmanned aerial vehicle, vessel and fiber will be required to operate jointly. Thus, the hybrid-channels QKD scheme can effectively address the key distribution requirements in specialized application scenarios.

At present, there are efforts[17–21] dedicated to researching the inter-modal operation of free-space and fiber channels. Specifically, Li *et al.*[21] first conducted a hybrid quantum communication network integrated free-space and fiber channels through Hong–Ou–Mandel interference, demonstrating the feasibility of inter-modal QKD network in full daytime. While this experimental MDI scheme requires maintaining the reference frame alignment, which significantly increases the complexity and difficulty of QKD experiments. Notice that reference-frame-independent measurement-device-independent QKD (RFI-MDI-QKD) proposed by Yin *et al.*,[22] offers an alternative approach without calibrating reference frame at all times. This protocol not only enables two parties to negotiate secure keys regardless of the reference frame misalignment but also effectively removes detector side channels. In experimental aspect, the proof-of-principle RFI-MDI-QKD experiment was presented by Wang *et al.*[23] These experimental advancements in RFI-MDI protocol[23–27] have not only validated the protocol's practicability but also demonstrated its inherent robustness against reference frame misalignment. Therefore, the RFI-MDI-QKD scheme in hybrid channels holds significant potential and deserves further investigation.

The paramount consideration in the theoretical analysis of RFI-MDI-QKD protocol performance in hybrid channels is that the transmittance depends on the weather conditions.[28] Due to the temporal fluctuations of the local refractive index in the free-space channel, the key characteristic of the free-space channel is its time-dependent transmittance.[29] Hence, the quantum bit error rate (QBER) of the QKD protocol changes

†Corresponding author. E-mail: winmaxsky@163.com

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

© 2025 Chinese Physical Society and IOP Publishing Ltd. All rights, including for text and data mining, AI training, and similar technologies, are reserved.

with time during the entire process of the experiment. In the previous literature, the secure key rate is derived in free-space links through various transmittance processing methods, including time-averaged channel,[30] numerical threshold optimization,[31] and adaptive real-time selection.[32] However these approaches impose significant data storage demands.

The prefixed-threshold real-time selection (P-RTS)[33] can relax the pressure on the data store through setting a transmittance threshold before conducting QKD experiment. This method has the great advantage of being able to predict the optimal threshold, regardless of the actual channel turbulence and loss condition. Advantage distillation techniques (ADT)[34–36] operate by performing preliminary processing on raw keys to reduce the QBER while enhancing the correlation between raw keys. In this paper, we apply P-RTS and ADT to RFI-MDI-QKD to enhance the protocol's performance in hybrid channels. We then analyze the influence of the P-RTS on decoy-state RFI-MDI-QKD in both asymptotic and nonasymptotic cases. According to the simulation results in the asymptotic case, we find that the performance of RFI-MDI-QKD protocol in hybrid channels is better than that in pure fiber channel. Although the average attenuation of fiber channel and free-space channel is the same, we can filter out some data with high transmission efficiency through the P-RTS in hybrid channels. Thus, the key rate calculated by filtered data is higher than unfiltered data. Under the condition of the nonasymptotic case, the result demonstrates that the maximum transmission distance can be improved by 15 km and 28 km when $N = 10^{12}$ and 10^{11} with P-RTS. Besides, the simulation results show that the Bob's maximum transmission distance is improved from 63 km to 76 km and from 96 km to 106 km, when $N = 10^{11}$ and 10^{12} with ADT for hybrid channels. Therefore, P-RTS and ADT make great sense to improve the maximal transmission distance and the maximal error rate tolerance for RFI-MDI-QKD via hybrid channels. Our work provides initial insights that could be factored into future hybrid channels QKD experimental designs.

2. Protocol

In this section, we first show the schematic diagram of implementing RFI-MDI-QKD in hybrid channels in Fig. 1. Our proposed model envisions a scenario where unmanned aerial vehicles, vessels, or similar apparatuses communicate with data processing centers or any desired terrestrial locations. This innovative scheme allows for seamless and continuous communication, particularly beneficial for emergency operations and missions conducted in the air or at sea. The advantage of this scheme is that it can realize the key refresh for unmanned aerial vehicles without landing and vessels without docking. Our model significantly enhances operational efficiency and security, providing a robust solution for real-time data exchange in critical situations. However, this scheme requires substantial advancements, with key technical challenges in synchronization, two-photon interference, and measurement yet to be addressed. In our paper, our research primarily focuses on how to efficiently distribute keys based on the theoretical framework in hybrid channels. Our aim is to enhance the robustness of the RFI-MDI-QKD protocol and optimize the efficiency of key generation processes. Next, a comprehensive model of RFI-MDI-QKD protocol tailored for hybrid channels with ADT is introduced.

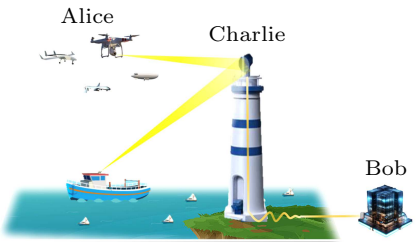


Fig. 1. Schematic diagram of implementing RFI-MDI-QKD in hybrid channels. Alice can be a unmanned aerial vehicle or a vessel. Charlie is a lighthouse as the measurement station to conduct Bell state measurement (BSM). Bob is a data processing center or any desired land location accessible by fiber.

Preparation Here, we denote a source on Alice's side by subscript A and on Bob's side by subscript B. In our protocol, Alice and Bob randomly choose Z basis, X basis and Y basis with equal probability. In each round, Alice (Bob) needs three different intensities from μ_a, ν_a, ω_a (μ_b, ν_b, ω_b) with probabilities $p_{\mu_a}, p_{\nu_a}, p_{\omega_a}$ ($p_{\mu_b}, p_{\nu_b}, p_{\omega_b}$), respectively. Then, Alice send her phase randomized weak coherent pulses to Charlie via free-space quantum channel and Bob via fiber channel.

Measurement and sifting Charlie conducts BSM for the received pulses, and then publishes his measurement result through a public channel. Both parties publicly compare their bases and intensity information for each pulse. Then both parties need to retain the events with the basis combination $d \in \{X_AX_B, X_AY_B, Y_AX_B, Y_AY_B, Z_AZ_B\}$. When using the same basis Z_AZ_B and with Charlie announcing a successful measurement result for the pulse pairs, Alice and Bob record the bit value as a raw key.

Parameter estimation Alice and Bob need to estimate the lower bound of single photon counting rate and calculate the upper bound of Eve's information I_E^{U} with the decoy-state method.

Advantage distillation Alice and Bob need to divide their raw key, which is kept in their hands, into b bits per block $\{x_0, x_1, \ldots, x_{b-1}\}$ and $\{y_0, y_1, \ldots, y_{b-1}\}$, respectively. Alice randomly generates a bit value $c \in \{0,1\}$ and performs an XOR operation with each bit in the key block, obtaining $M_A = \{m_0, m_1, \ldots, m_{b-1}\} = \{x_0 \oplus c, x_1 \oplus c, \ldots, x_{b-1} \oplus c\}$. Then, the computed results M_A are sent to Bob through an authenticated channel. For receiving M_A, Bob also conducts XOR operation

$M_B = \{y_0 \oplus m_0, y_1 \oplus m_1, \ldots, y_{b-1} \oplus m_{b-1}\}$. They accept the block if and only if $M_B = \{0,0,\ldots,0\}$ or $M_B = \{1,1,\ldots,1\}$, otherwise they discard the block. For the accepting block, Alice and Bob only keep the first bit x_0 and y_0 as the raw key.

Post-processing Both parties implement an error correction algorithm to ensure that their corrected keys are identical. Finally, based on the information leaked to the eavesdropper, the privacy amplification compresses their keys to a certain.

The secret key rate of RFI-MDI-QKD in the asymptotic case can be expressed as[34,44]

$$R \geq Q_{\mu_a\mu_b}^{Z_AZ_B}\left[\frac{Y_{11}^{Z_AZ_B}P_{11}}{Q_{\mu_a\mu_b}^{Z_AZ_B}}\left(1-(\varphi_0+\varphi_1)H\left(\frac{\varphi_0}{\varphi_0+\varphi_1}\right)-(\varphi_2+\varphi_3)H\left(\frac{\varphi_2}{\varphi_2+\varphi_3}\right)\right)-fH\left(E_{\mu_a\mu_b}\right)\right], \quad (1)$$

where $Q_{\mu_a\mu_b}^{Z_AZ_B}$ is the overall gain of Alice and Bob sending quantum states with intensities μ_a and μ_b in the combination of Z_AZ_B basis, respectively. $Y_{11}^{Z_AZ_B}$ is the single-photon counting rate with the combination of Z_AZ_B basis, φ_i is related to the single photon error rate, P_{11} is the probability that both Alice and Bob prepare a quantum state with a single photon, $H(x) = -x\log_2 x-(1-x)\log_2(1-x)$ is the binary entropy function, $E_{\mu_a\mu_b}$ is the overall error rate in the signal quantum states.

3. Theorem and method for RFI-MDI-QKD

3.1. Atmospheric effects

The quantum states of light in free-space are affected by fluctuating losses, which follow the PDT. There have been multiple efforts to accurately characterize the PDT, such as analytical models: the log-normal distribution,[29] the beam wandering model,[37] the elliptic-beam approximation,[38] and the model based on the law of total probability.[39] Their applicability is shown to strongly depend on the receiver aperture radius and slightly dependent on the turbulence strength.[40] Besides, they are cumbersome to handle, even numerically, and therefore restrictive for a theoretical account of the practical system. Therefore, it is difficult to choose the best PDT model for characterizing the features of atmospheric turbulence in practical free-space channel. Fortunately, the Beta distribution model fits the results of numerical simulation better than other analytical models for a wide range of channel parameters.[40] Therefore, we choose the Beta model for characterizing the features of fluctuating atmospheric turbulence. Specifically, the Beta distribution model is shown below:

$$P(\eta) = \frac{1}{B(\gamma_a,\gamma_b)}\eta^{\gamma_a-1}(1-\eta)^{\gamma_b-1}, \quad (2)$$

where $B(\gamma_a,\gamma_b)$ is the Beta function, γ_a and γ_b are related to parameters $\langle\eta\rangle$ and σ, which are inherent to the channel itself. $\langle\eta\rangle$ is the average transmission efficiency. σ is determined by the amount of turbulence, typically taking a value between zero and one. Thus, the pair $(\langle\eta\rangle,\sigma)$ contains all information of the PDTC. Then, the parameters γ_a and γ_b of the Beta probability distribution are

$$\gamma_a = \gamma_a(\langle\eta\rangle,\sigma) = \frac{1-\langle\eta\rangle(1+\sigma^2)}{\sigma^2}, \quad (3)$$

$$\gamma_b = \gamma_b(\langle\eta\rangle,\sigma) = \gamma_a(\langle\eta\rangle,\sigma)\left(\frac{1}{\langle\eta\rangle}-1\right). \quad (4)$$

3.2. Improved the secret key rate with ADT

Given that the ADT operates purely through software-based parameter optimization without requiring modifications to existing quantum state preparation or measurement hardware, we explore its potential to enhance the RFI-MDI-QKD protocol's performance in hybrid channels. Furthermore, due to the limitations of atmospheric turbulence, it is difficult to collect some high-quality data that can be used to extract the keys. Then, ADT performs preliminary processing on raw keys to reduce the QBER while enhancing the correlation between raw keys. Thus, ADT has the potential to enhance the maximum tolerable QBER, enhancing the performance of RFI-MDI-QKD through information reconciliation. Thus, by combining the decoy-state method, the successful probability of the ADT can be expressed as

$$p_{\text{succ}} = \left(E_{\mu_a\mu_b}\right)^b + \left(1-E_{\mu_a\mu_b}\right)^b, \quad (5)$$

then the overall error rate after advantage distillation step is given by

$$\tilde{E}_{\mu_a\mu_b} = \frac{\left(E_{\mu_a\mu_b}\right)^b}{\left(E_{\mu_a\mu_b}\right)^b + \left(1-E_{\mu_a\mu_b}\right)^b}. \quad (6)$$

Meanwhile, the single photon error rate is given by

$$p_{\text{s}} = \left(e_{11}^{Z_AZ_B}\right)^b + \left(1-e_{11}^{Z_AZ_B}\right)^b, \quad (7)$$

where e_{11} is the single photon error rate, and b is the step size of advantage distillation, which must be an integer greater than or equal to 1. The other parameters satisfy

$$\tilde{\varphi}_0 = \frac{(\varphi_0+\varphi_1)^b+(\varphi_0-\varphi_1)^b}{2p_{\text{s}}},$$

$$\tilde{\varphi}_1 = \frac{(\varphi_0+\varphi_1)^b-(\varphi_0-\varphi_1)^b}{2p_{\text{s}}},$$

$$\tilde{\varphi}_2 = \frac{(\varphi_2+\varphi_3)^b+(\varphi_2-\varphi_3)^b}{2p_{\text{s}}},$$

$$\tilde{\varphi}_3 = \frac{(\varphi_2+\varphi_3)^b-(\varphi_2-\varphi_3)^b}{2p_{\text{s}}}, \quad (8)$$

$$\tilde{C} = 2\left[(\tilde{\varphi}_0-\tilde{\varphi}_1)^2+(\tilde{\varphi}_2-\tilde{\varphi}_3)^2\right], \quad (9)$$

$$\tilde{v} = \frac{1}{(\tilde{\varphi}_2+\tilde{\varphi}_3)}\sqrt{\frac{\tilde{C}}{2}-(\tilde{\varphi}_0+\tilde{\varphi}_1)^2\tilde{u}_{\max}^2}, \quad (10)$$

$$\tilde{u}_{\max} = \min\left[\frac{1}{\tilde{\varphi}_0+\tilde{\varphi}_1}\sqrt{\frac{\tilde{C}}{2}},\ 1\right]. \tag{11}$$

By combining the three-intensities decoy-state RFI-MDI-QKD scheme[45] and ADT,[34] the final secret key rate of the decoy-state RFI-MDI-QKD protocol after advantage distillation step can be expressed as[36]

$$\begin{aligned} R^b \geq \max_b \min_{\{\varphi_0,\varphi_1,\varphi_2,\varphi_3\}} & \frac{1}{b} p_{\text{succ}} Q_{\mu_a\mu_b}^{Z_AZ_B} \\ & \times \left[\left(\frac{Y_{11}^{Z_AZ_B}P_{11}}{Q_{\mu_a\mu_b}^{Z_AZ_B}}\right)^b \left(1-(\tilde{\varphi}_0+\tilde{\varphi}_1)^b H\left(\frac{1+\tilde{u}}{2}\right)\right.\right. \\ & \left.\left. -(\tilde{\varphi}_2+\tilde{\varphi}_3)^b H\left(\frac{1+\tilde{v}}{2}\right)\right) - fH\left(\tilde{E}_{\mu_a\mu_b}\right)\right]. \end{aligned} \tag{12}$$

The above analysis is based on the infinite length of pulse pairs. However, we must consider the scenario where the length of sending pulses is finite in a practical QKD system. Next, the statistical fluctuation analysis will be considered. The secret key rate of the RFI-MDI-QKD protocol when taking statistical fluctuation into account can be expressed as

$$\begin{aligned} R_N^b \geq \max_b \min_{\{\varphi_0,\varphi_1,\varphi_2,\varphi_3\}} & \frac{1}{Nb} p_{\text{succ}} n_{\mu_a\mu_b}^{Z_AZ_B} \\ & \times \left[\left(\frac{\langle s_{11}^{Z_AZ_B,\text{L}}\rangle}{n_{\mu_a\mu_b}^{Z_AZ_B}}\right)^b \left(1-(\tilde{\varphi}_0+\tilde{\varphi}_1)^b H\left(\frac{1+\tilde{u}}{2}\right)\right.\right. \\ & \left.\left. -(\tilde{\varphi}_2+\tilde{\varphi}_3)^b H\left(\frac{1+\tilde{v}}{2}\right)\right) - fH\left(\tilde{E}_{\mu_a\mu_b}\right)\right], \end{aligned} \tag{13}$$

where N denotes the total number of transmitted pulse pairs, $n_{\mu_a\mu_b}^{Z_AZ_B}$ is the total number of detection counts given that Alice and Bob both sent quantum states with $\mu_a\mu_b$ intensity in the combination of Z_AZ_B basis. $\langle s_{11}^{Z_AZ_B,\text{L}}\rangle$ is the lower bound of $\langle s_{11}^{Z_AZ_B}\rangle$, which is the number of successful measurement events where Alice and Bob both sent single-photon states in the combination of Z_AZ_B basis. The detailed decoy-state method can be referred to Ref. [36]. In addition to analyzing the misalignment of the reference frame, due to the imperfection of devices, the condition for mutually unbiased bases may not be satisfied. Subsequently, we can integrate the theories of reference frame independent and virtual mutually unbiased bases[46] to further enhance the QKD protocol.

When both Alice and Bob transmit quantum states via fiber channel, the key rate can be formulated as follows:

$$R_{\text{fiber}} = R(\langle\eta_a\rangle, \eta_b, \beta), \tag{14}$$

where β is the deviation angle of the reference frame, $\langle\eta_a\rangle$ is Alice's overall transmittance efficiency and η_b is the total transmittance for Bob, including the optical system efficiency and the detector's efficiency.

3.3. Maximizing the secret key rate in fiber–atmospheric channels

Here, we consider the scenario where Alice and Bob transmit quantum states via fluctuating free-space channel and stable fiber channel, respectively. Assuming that we have complete knowledge of the statistical properties of the free-space channel with the technology of real-time transmittance detection, we can get the channel transmittance η when each quantum state passes through the free-space channel. Then, these signals can be ordered from low to high transmittance η. The range of transmittance η is from zero to one, dividing the interval $[0,1]$ into n sub-intervals. The length of each sub-interval is $\Delta\eta_1 = \eta_1 - \eta_0$, $\Delta\eta_2 = \eta_2 - \eta_1$, …, $\Delta\eta_n = \eta_n - \eta_{n-1}$. Therefore, we can assume that these signals pass through the free-space channel with the same transmittance η for each sub-interval $[\eta, \eta+\Delta\eta)$. To put it differently, signals residing in the same sub-interval can be regarded as being in a "static channel", thereby enabling the application of the identical rate formula $R(\eta)$ and security analysis as if η were a fixed constant.

Then, we can calculate the number of secure key bits from each sub-interval, and add all sub-intervals together. When $\max\{\Delta\eta_1, \Delta\eta_2, \ldots, \Delta\eta_n\} \to 0$, this is an integration of $R(\eta)$ over η with $P(\eta)$ being the weight. Therefore, the total key rate of the RFI-MDI-QKD system as the weight average over all possible values of η in free-space and fiber-integrated channels satisfies

$$R''_{\text{hybrid}} = \int_0^1 R(\eta_a, \eta_b, \beta) P(\eta_a)\, \mathrm{d}\eta_a, \tag{15}$$

where η_a is the real-time fluctuating total transmittance. This approach for computing the key rate, called the ratewise integration,[33] utilizes the full information of the transmittance probability distribution.

Usually, the probability of bit errors occurring in the transmitted signals is higher when the channel's transmission efficiency is low. Then, the process of key negotiation will be terminated if the bit error rate surpasses the value of the prefixed security threshold. Thus, we can calculate a threshold η_{T} before conducting the RFI-MDI-QKD experiment in hybrid channels. These signals are simply discarded if the instantaneous transmission efficiency of the real-time monitoring channel falls below η_{T}. Actually, these signals have no contribution to the final secure keys. Then, we can predefine a threshold η_{T} in the ratewise integration model, the key rate can be given by

$$R'_{\text{hybrid}} = \int_{\eta_{\text{T}}}^1 R(\eta_a, \eta_b, \beta) P(\eta_a)\, \mathrm{d}\eta_a. \tag{16}$$

We adopt the simplified method proposed in Ref. [33] that gives the key rate using only the average transmittance of the

postselected signals as follows:

$$\tilde{\eta}_a = \frac{\int_{\eta_T}^{1} \eta_a P(\eta_a)\,\mathrm{d}\eta_a}{\int_{\eta_T}^{1} P(\eta_a)\,\mathrm{d}\eta_a}, \tag{17}$$

$$R_{\text{hybrid}} = \int_{\eta_T}^{1} P(\eta_a)\,\mathrm{d}\eta_a \times R(\tilde{\eta}_a, \eta_b, \beta). \tag{18}$$

Due to the impracticality of obtaining an infinite number of pulses in QKD systems, the length of the secret key is generally finite. Considering the finite pulses, the key rate is as follows:

$$R^N_{\text{hybrid}} = \int_{\eta_T}^{1} P(\eta_a)\,\mathrm{d}\eta_a \times R_N\left(\tilde{\eta}_a, \eta_b, \beta, N\int_{\eta_T}^{1} P(\eta_a)\,\mathrm{d}\eta_a\right), \tag{19}$$

which implies that postselection has a double impact on the key rate of RFI-MDI-QKD protocol in nonasymptotic case. It not only affects the overall rate due to the portion of lost signals but also decreases the signal number N used to actually perform the protocol, which causes higher statistical fluctuations. While this method is promising in reducing the data processing burden and has been applied to the free-space MDI-QKD,[47] RFI-QKD[48] and sending or not sending QKD.[49] Next, we need to seek η_T through simulation with and without ADT for the RFI-MDI-QKD protocol. Furthermore, the robustness against the deviation of the reference frame is another significant problem when employing this simplified method.

4. Numerical simulation

In this section, we implement the aforementioned models to evaluate the performance of RFI-MDI-QKD in hybrid channels and fiber-only channel in both asymptotic and nonasymptotic cases. Here, we first set the experimental parameters that may be used. Then, we analyze and discuss our simulation results. The parameters are listed in Table 1.

Table 1. List of practical parameters employed in our numerical simulation.

Variable	Parameter	Simulation value
p_d	dark count rate	6.02×10^{-6}
α	fiber loss coefficient (dB/km)	0.2
η_E	efficiency of experimental apparatuses	0.145
e_d	intrinsic misalignment error	1.5%
f	efficiency of error correction	1.16

In Fig. 2, we present the performance of infinite length pulses. We compare the performance of RFI-MDI-QKD between hybrid channels and fiber-only channel. Here, Bob's fiber channel is configured with 30 km, while Alice's average attenuation is set to 15 dB. For the hybrid channels, the average attenuation of the free-space channel is 15 dB, and the atmospheric turbulence variance is set to 0.6, corresponding to $(\langle\eta\rangle = 0.0316, \sigma = 0.6)$. The blue solid line denotes the performance in accordance with utilizing all information of PDT. The dashed line represents the scenario where all quantum states are transmitted over stable fiber channel for Alice and Bob. The red solid line, representing the key rate calculated by the simplified method, varies with the increase of prefixed-threshold η_T and reaches its climax at the point of $\eta_T = 0.018586$. The maximum key rate calculated by the simplified method is close to the performance of utilizing all information of PDT. In the process of initially raising the threshold, the signal with high transmittance is filtered out to improve the average transmittance of the system. When the threshold is further increased, the total number of signals will decrease significantly if the detection threshold is too high, resulting in the decrease of the key rate. In addition, the performance of the RFI-MDI-QKD protocol in hybrid channels is better than that in pure fiber channel. The main reason is that transmittance fluctuates due to atmospheric turbulence. Although the average attenuation of fiber channel and free-space channel is the same, we can filter out some data with high transmission efficiency through the P-RTS. Thus, the key rate calculated by filtered data is better than unfiltered data.

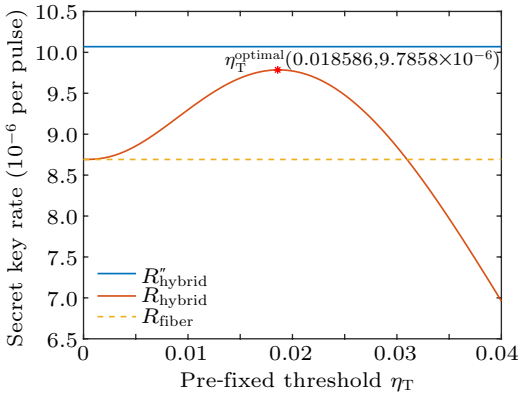


Fig. 2. Comparison of the ratewise integration model R''_{hybrid} and P-RTS model R_{hybrid} versus fiber-only channel R_{fiber} for RFI-MDI-QKD when considering infinite-length pulses.

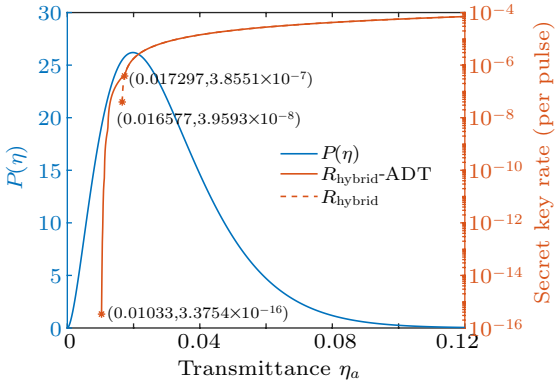


Fig. 3. The RFI-MDI-QKD rate and PDT versus transmittance η_a with and without ADT.

In Fig. 3, we present the performance of RFI-MDI-QKD with and without ADT in the asymptotic case. The red solid line corresponds to the results with ADT, and the red dashed

line denotes the results without ADT. The blue line represents the fluctuations of the free-space atmospheric link, corresponding to $(\langle\eta\rangle = 0.0316, \sigma = 0.6)$. And a 30 km fiber optic channel is designated for Bob. We can find that the minimum acceptable transmission efficiency is improved from 0.016 to 0.01. Thus, the ADT can improve tolerable atmospheric attenuation. This means that more data can be collected to generate keys if ADT is utilized in practical QKD experiment. The significant implication is that as long as we know the experimental parameters, we can determine the threshold in advance, without the need to know any information about the channel. It will substantially reduce the amount of data storage requirements in the experiment, since Charlie does not need to store all data until after experiment for optimization of threshold.

As illustrated in Fig. 4(a), we compare scenarios regarding free-space channel η_a as a statistical constant and utilizing the information of the PDT for different total number transmitted pulses N. Here, Alice's average attenuation is fixed to 8 dB and $\sigma = 0.5$ for the free-space channel. The solid lines are results with employing the P-RTS method. The dashed lines are results regarding Alice's free-space channel η_a as a statistical constant. This is to say, Alice and Bob transmit the quantum states via fiber channel. We can find that by making full use of the transmission efficiency fluctuations introduced by atmospheric turbulence, the maximum transmission distance can be improved by 15 km and 28 km when $N = 10^{12}$ and 10^{11}. The result demonstrates that with the condition of statistical fluctuations, utilizing the P-RTS can improve the performance of RFI-MDI-QKD in hybrid channels compared to fiber-only channel.

Then, we analyze the effect of the ADT on RFI-MDI-QKD for the nonasymptotic case under hybrid channels in Fig. 4(b). Here, we set the total number of transmitted pulses $N = 10^{11}$ and 10^{12}. The solid lines represent the results without ADT. The dotted lines represent the results with ADT. We can find that Bob's maximum transmission distance is improved from 63 km to 76 km and from 96 km to 106 km when $N = 10^{11}$ and 10^{12}. The main reason is that the influence of statistical fluctuation caused by finite-length pulse will seriously reduce the estimation of single photon count rate and increase the estimation of single photon bit error rate. With the general QKD security framework, no keys will be distributed if the single photon bit error rate exceeds a certain threshold. The main idea of ADT is to divide the raw keys into blocks, identify the highly correlated bit subset and separate it from the weakly correlated information. Thus, the QBER of the selected data is reduced. Therefore, ADT can improve the RFI-MDI-QKD protocol's performance.

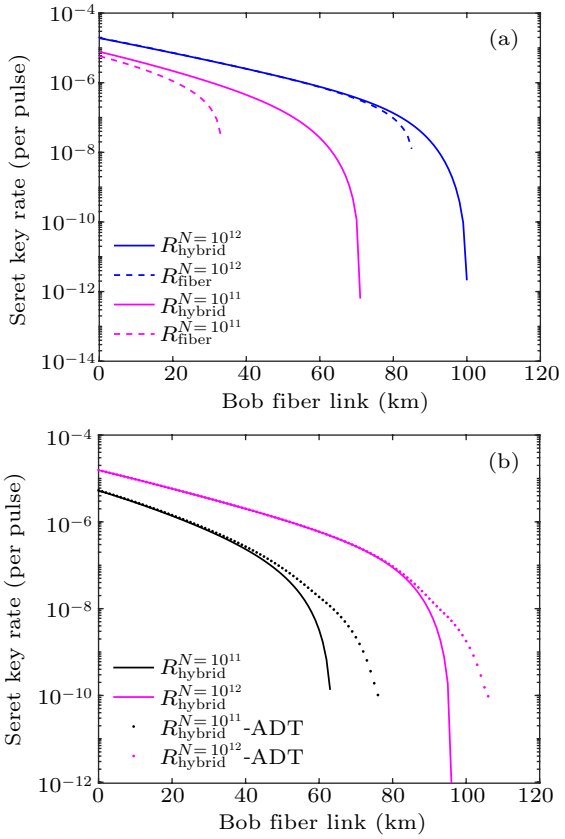


Fig. 4. The secret key rate (per pulse) in logarithmic scale versus Bob's transmission distance with Alice's average attenuation fixed to 8 dB and $\sigma = 0.5$ in the decoy-state RFI-MDI-QKD and different total numbers of transmitted pulses $N = 10^{11}$ and 10^{12}. (a) Comparsion of the hybrid channels model and fiber-only channels. (b) Comparsion of the hybrid channels model with and without ADT.

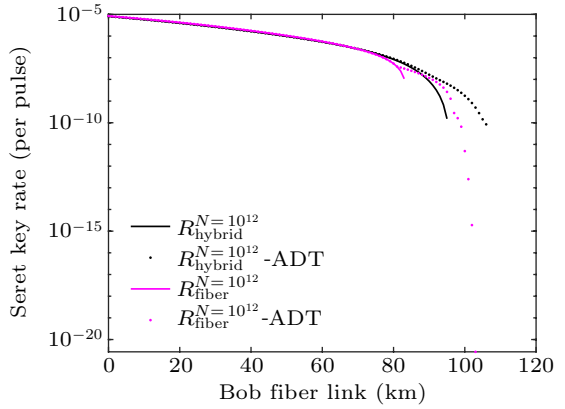


Fig. 5. The secret key rate (per pulse) in logarithmic scale versus Bob's transmission distance with reference frame misalignment fixed at $\beta = \pi/9$.

In order to further analyze the facilitation of the ADT in the nonasymptotic case, we consider the reference frame misalignment and different channel types. Here, Alice's average attenuation is fixed to 8 dB and $\sigma = 0.5$ for free-space channel. The solid lines are results without the ADT ($b = 1$) and dotted lines are results with the ADT ($b > 1$). From Fig. 5, it is clear that the performance of RFI-MDI-QKD can be improved with the ADT. Specially, the pink lines represent the scenario that Alice and Bob transmit quantum states via fiber channels. The black lines represent the scenario that Alice transmits quantum

states via free-space channel and Bob via fiber channel. From the simulation results, we can find that Bob's maximum fiber transmission distance can be improved by 20 km for fiber-only channel, 10 km for hybrid channels, when there is a reference frame misalignment of $\pi/9$ in the nonasymptotic scenario of $N = 10^{12}$. The main reason is that P-RTS has made the initial selection of the data, so the enhancement effect is not as good as the pure fiber channel.

From simulation results presented above, we can find that neglecting free-space fluctuations, the performance of RFI-MDI-QKD is the least satisfactory for fiber-only. The performance is optimal when the turbulent atmospheric can be accurately characterized. The P-RTS method offers a significant advantage by alleviating the strain on data storage requirements, which is beneficial for these scenarios where data storage is a critical consideration. Besides, the ADT profoundly affects both maximum transmission distance and the key rate when the key length is finite. Therefore, combining ADT and P-RTS not only improves the performance of RFI-MDI-QKD protocol but alleviates the demands on data storage in hybrid channels.

5. Conclusions

Considering the fluctuation of channel transmittance with time, we apply P-RTS and ADT to RFI-MDI-QKD to enhance the protocol's performance in hybrid channels. The scheme determines an appropriate threshold in advance through an optimization method and then filters out the signals with high transmittance to improve the key rate. It is worth noting that P-RTS method is only applicable to the fluctuating free space channel. From the simulation results, the feasibility of improving the performance of RFI-MDI-QKD using the P-RTS in hybrid channels has been verified. The maximum loss tolerance of RFI-MDI-QKD in turbulent conditions is markedly improved, while simultaneously retaining the intrinsic advantage of RFI-MDI-QKD against reference frame deviations. The effectiveness of the ADT in practical decoy-state implementations of RFI-MDI-QKD has been shown. Based on our work, it not only provides a more robust key distribution protocol but also establishes a solid theoretical foundation for improving the performance of RFI-MDI-QKD in hybrid channels.

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 Natural Science Foundation of Henan Province (Grant Nos. 202300410534 and 202300410534), and the Anhui Initiative in Quantum Information Technologies.

References

[1] Liao S K, Cai W Q, Handsteiner J, *et al.* 2018 *Phys. Rev. Lett.* **120** 030501
[2] Zhang Q, Xu F H, Chen Y A, *et al.* 2018 *Opt. Express* **26** 24260
[3] Gibney E 2016 *Nature* **535** 478
[4] Chen J P, Zhang C, Liu Y C, *et al.* 2020 *Phys. Rev. Lett.* **124** 070501
[5] Liu H, Jiang C, Zhu H T, *et al.* 2021 *Phys. Rev. Lett.* **126** 250502
[6] Wang S, Yin Z Q, He D Y, *et al.* 2022 *Nat. Photon.* **16** 154
[7] Liu Y, Zhang W J, Jiang C, *et al.* 2023 *Phys. Rev. Lett.* **130** 210801
[8] Liao S K, Cai W Q, Liu W Y, *et al.* 2017 *Nature* **549** 43
[9] Yin J, Cao Y, Li Y H, *et al.* 2017 *Phys. Rev. Lett.* **119** 200501
[10] Yin J, Li Y H, Liao S K, *et al.* 2020 *Nature* **582** 501
[11] Maeda K, Sasaki T and Koashi M 2019 *Nat. Commun.* **10** 3140
[12] Li W T, Wang L, Li W, *et al.* 2022 *Chin. Phys. B* **31** 050310
[13] Xie Y M, Lu Y S, Weng C X, *et al.* 2022 *PRX Quantum* **3** 020315
[14] Ju X X, Zhong W, Sheng Y B, *et al.* 2022 *Chin. Phys. B* **31** 100302
[15] Sun M, Zhang C M, Zhang R, *et al.* 2024 *Chin. Phys. B* **33** 110302
[16] Yang K X, Mao Y L, Chen H, *et al.* 2020 *Phys. Rev. Lett.* **133** 210803
[17] Liao S K, Yong H L, Liu C, *et al.* 2017 *Nat. Photonics* **11** 509
[18] Gong Y H, Yang K X, Yong H L, *et al.* 2018 *Nat. Photonics* **26** 18897
[19] Avesani M, Calderaro L, Schiavon M, *et al.* 2021 *npj Quantum Inf.* **7** 93
[20] Chen Y A, Zhang Q, Chen T Y, *et al.* 2021 *Nature* **589** 214
[21] Li Y H, Li S L, Hu X L, *et al.* 2023 *Phys. Rev. Lett.* **131** 100802
[22] Yin Z Q, Wang S, Chen W, *et al.* 2014 *Quantum Inf. Process.* **13** 1237
[23] Wang C, X. Song T, Yin Z Q, *et al.* 2015 *Phys. Rev. Lett.* **115** 160502
[24] Wang C, Yin Z Q, Wang S, *et al.* 2017 *Optica* **4** 1016
[25] Zhang C M, Zhu J R and Wang Q 2017 *Phys. Rev. A* **95** 032309
[26] Zhou X Y, Ding H J, Sun M S, *et al.* 2021 *Phys. Rev. Appl.* **15** 064016
[27] Fan-Yuan G J, Lu F Y, Wang S, *et al.* 2022 *Optica* **9** 812823
[28] Vasylyev D Y, Semenov A, Vogel W, *et al.* 2017 *Phys. Rev. A* **96** 043856
[29] Semenov A and Vogel W 2009 *Phys. Rev. A* **80** 021802
[30] Schmitt-Manderbach T, Weier H, Fürst M, *et al.* 2007 *Phys. Rev. Lett.* **98** 010504
[31] Erven C, Heim B, Meyer-Scott E, *et al.* 2012 *New J. Phys.* **14** 123018
[32] Vallone G, Marangon D G, Canale M, *et al.* 2015 *Phys. Rev. A* **91** 042320
[33] Wang W Y, Xu F H and Lo H K 2018 *Phys. Rev. A* **97** 032337
[34] Li H W, Zhang C M, Jiang M S, *et al.* 2022 *Commun. Phys.* **5** 53
[35] Zhu J R, Zhang C M, Wang R, *et al.* 2023 *Opt. Lett.* **48** 542545
[36] Jiang X L, Wang Y, Li J J, *et al.* 2023 *Opt. Express* **31** 9196
[37] Vasylyev D Y, Semenov A and Vogel W 2012 *Phys. Rev. Lett.* **108** 220501
[38] Vasylyev D Y, Semenov A and Vogel W 2016 *Phys. Rev. Lett.* **117** 090501
[39] Vasylyev D Y, Vogel W and Semenov A 2018 *Phys. Rev. A* **97** 063852
[40] Klen M and Semenov A 2023 *Phys. Rev. A* **108** 033718
[41] Andrews L C and Phillips R L 2005 *Laser Beam Propagation Through Random Media* 2nd Edn.
[42] Ricklin J C, Hammel S M, Eaton F D, *et al.* 2006 *J. Opt. Fiber Commun. Reports* **3** 111
[43] Lu Q H, Wang F X, Chen W, *et al.* 2024 *Sci. China Inf. Sci.* **67** 142503
[44] Gottesman D, Lo H K, Lükenhaus N *et al.* 2004 *Internation Symposium onInformation Theory IEEE* 136
[45] Lu F Y, Yin Z Q, Fan-Yuan G J, *et al.* 2020 *Phys. Rev. A* **101** 052318
[46] Li H W, Hao C P, Chen Z J, *et al.* 2024 *Sci. China-Phys. Mech. Astron.* **67** 270313
[47] Zhu Z D, Chen D, Zhao S H, *et al.* 2019 *Quantum Inf. Process.* **18** 1
[48] Xue Y, Shi L, Chen W, *et al.* 2020 *Phys. Rev. A* **102** 062602
[49] Yu Y, Xu R, Wang L, *et al.* 2022 *Entropy* **24** 344