entropy

MDPI

Article

Free Space Measurement Device Independent Quantum Key Distribution with Modulating Retro-Reflectors under Correlated Turbulent Channel

Xingyu Wang [1,2,†], Wei Liu [1,†], Tianyi Wu [1], Chang Guo [1], Yijun Zhang [1,3], Shanghong Zhao [2] and Chen Dong [1,*]

[1] Information and Communication College, National University of Defense Technology, Xi'an 710006, China; wang_kgd@foxmail.com (X.W.); liuwei0927@126.com (W.L.); wutianyi13@nudt.edu.cn (T.W.); gxcy185@163.com (C.G.); gfkd_zyj@163.com (Y.Z.)
[2] School of Information and Navigation, Air Force Engineering University, Xi'an 710077, China; zhaoshangh@aliyun.com
[3] Graduate Institute, Rocket Force University of Engineering, Xi'an 710025, China
* Correspondence: dongchengfkd@163.com
† These authors contributed equally to this work.

Abstract: Modulating retro-reflector (MRR), originally introduced to support laser communication, relieves most of the weight, power, and pointing requirements to the ground station. In this paper, a plug-and-play measurement device independent quantum key distribution (MDI-QKD) scheme with MRR is proposed not only to eliminate detector side channels and allow an untrusted satellite relay between two users, but also to simplify the requirements set-ups in practical flexible moving scenarios. The plug-and-play architecture compensates for the polarization drift during the transmission to provide superior performance in implementing the MDI-QKD on a free-space channel, and the MRR device is adopted to relax the requirements on both communication terminals. A double-pass correlated turbulent channel model is presented to investigate the complex and unstable channel characteristics caused by the atmospheric turbulence. Furthermore, the security of the modified MDI-QKD scheme is analyzed under some classical attacks and the simulation results indicate the feasibility under the situation that the system performance deteriorates with the increase of fading correlation coefficient and the turbulence intensity, which provides a meaningful step towards an MDI-QKD based on the moving platforms to join a dynamic quantum network with untrusted relays.

Keywords: MDI-QKD; modulating retro-reflector; double-pass channel; atmosphere turbulence

Citation: Wang, X.; Liu, W.; Wu, T.; Guo, C.; Zhang, Y.; Zhao, S.; Dong, C. Free Space Measurement Device Independent Quantum Key Distribution with Modulating Retro-Reflectors under Correlated Turbulent Channel. *Entropy* **2021**, *23*, 1299. https://doi.org/10.3390/e23101299

Academic Editors: Leong Chuan Kwek, Xiang-Bin Wang and Cong Jiang

Received: 6 August 2021
Accepted: 26 September 2021
Published: 1 October 2021

1. Introduction

Measurement device independent quantum key distribution (MDI-QKD) [1], which is immune to all attacks against the detection system and allows a QKD network with untrusted relays, has been a promising area to guarantee the information security of communications [2–4]. Recently, the fiber-based implementations rapidly developed towards longer distance [5–7], and higher key rates [8,9]. However, the implementation of MDI-QKD requires the indistinguishability of the spectral, polarization and temporal modes of the photons from Alice and Bob, which is much more difficult to manipulate under a free space channel than a fiber-based channel because the free-space optical channels dramatically fluctuate, caused by the atmospheric turbulence [10].

An achievement of the free-space MDI-QKD experiment was made in [11], which paves a significant step towards the satellite-based MDI-QKD [12] or other QKD applications [13]. However, the links in these experiments are relatively fixed while in the satellite-to-ground scenario they are dynamic and flexible [14]. In addition, the observation of high-visibility Hong-Ou-Mandel (HOM) interference requires the indistinguishability of optical pulses that are generated by two independent photon sources and transmitted through two independent free-space channels, which is a big challenge to share the time and frequency via free-space links.

Recently, inspired by the multidirectional links using the modulating retro-reflector (MRR) for high rate free-space optical communication [15], a laboratory-based free-space QKD with the MRR setting was presented in [16], which can ease the pointing requirements and maintain the narrow beam divergence necessary for long-range communication links. Meanwhile, the fading channel of double-pass MRR free-space optical (FSO) systems under weak turbulence conditions is investigated in [17], which can be modeled by the distribution of the weighted product of two correlated Log-normal random variables. These research results lay a foundation for extending the MRR device to the MDI-QKD scheme, which can be a desirable yet highly challenging application towards future free-space MDI-QKD experiments.

In this paper, a plug-and-play MDI-QKD scheme with modulating retro-reflectors is proposed not only to inherit the merit of the structure, where the plug-and-play architecture compensates for the polarization drift during the transmission to provide superior performance in implementing the MDI-QKD on free space channel, but also to bring advantages of the MRR device, which is adopted in classical free space communication system to relax the requirements on both communication terminals. Then, considering that the fading of the two passes is correlated in the double-pass scheme, a correlated turbulent channel model for the double-pass MRR QKD link is used to investigate the turbulence effect on the key generation rate and the QBER. Furthermore, the security of the modified MDI-QKD scheme is analyzed under some classical attacks. The simulation results indicate the feasibility of the modified MDI-QKD scheme under the situation that the system performance deteriorates with the increase of the fading correlation coefficient and the turbulence intensity, which is a meaningful step to make our modified MDI-QKD with MRR suitable for mobile scenarios with flexible deployment.

The organization of the article is as follows. In Section 2, we present the concept of the free-space MDI-QKD with modulating retro-reflectors and introduce the different features in the process of the “Preparation” and “Measurement”. Then, in Section 3, the channel of the double-pass MRR-MDI-QKD link under turbulence is modeled, and the key rate of MRR-MDI-QKD is estimated by combining the correlated Log-normal distribution model and the decoy-state QKD method. In Section 4, we simulated the performance of the involved MRR-MDI-QKD. We concluded this paper in Section 5. The article is ended in with a security analysis of the MRR-MDI-QKD.

2. The Concept of the Free-Space MDI-QKD with Modulating Retro-Reflectors

The schematic diagram of our MRR-MDI-QKD model is shown in Figure 1. Different from the traditional MDI-QKD scheme using two laser sources from Alice and Bob respectively, the plug-and-play MDI-QKD [18] scheme with the MRR only adopts a single laser source held by Charlie, which naturally solves the problem of spectrum matching owing to the independent photon preparation process. The preparation process is achieved by using MRR and polarization beam splitters (PBS) acting on the input pulses at Alice and Bob independently and reflect the polarization-encoded photon back to Charlie to perform the measurement. The Bell state measurement (BSM) procedure is the same as the traditional MDI-QKD scheme.

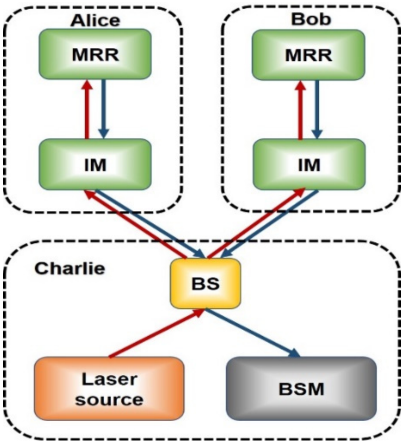
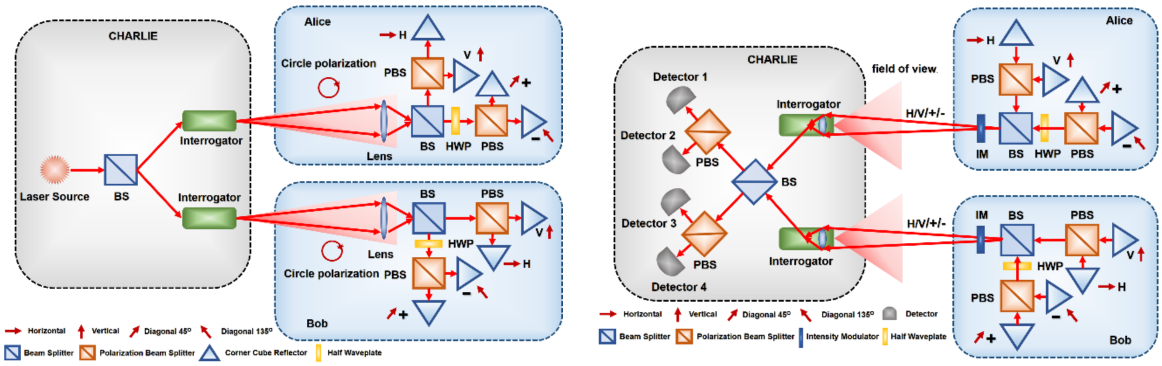


Figure 1. Schematic Diagram of the MDI-QKD with MRR. IM: Intensity Modulator; MRR: Modulating Retro-Reflectors; BSM: Bell State Measurement; BS: Beam Splitters.

Similar to the original MDI-QKD protocol, Charlie sends a laser pulse through BS to split two beams into the input of interrogator. As shown in Figure 2a, the circle polarization beam sends to Alice and Bob to perform the encode process respectively.



(**a**) Experimental of Preparation Set-ups (**b**) Experimental of Bell State Measurement Set-ups

Figure 2. The schematic diagram of the MDI-QKD with MRR.

Take the experimental apparatus of the upper part as an example; the circularly polarized beam enters Alice's set-up diagram and is divided into two paths by a beam splitter. In the path for the H-V basis where $|H\rangle$ and $|V\rangle$ refer to the horizontal and vertical polarization directions, respectively, the circularly polarized beam is split into horizontal and vertical components by a polarizing beam-splitter. Alice changes the strength of transmission state of MRR to encode the H-V basis on reflected light. The process is driven by a random data signal consisting of a binary one and zero, where the modulator is driven to its high transmission state when the data consists of a binary one and the modulator is driven to its low transmission state when the data consists of a binary zero. In the path for the diagonal basis, where $|+\rangle$ and $|-\rangle$ $|-\rangle$ denote 45-degree and 135-degree diagonal polarization directions, Alice only needs to use half-wave plates (HWP) to apply polarization rotations to implement the process. Thus, Alice and Bob use the MRR to randomly choose a basis from $\{|H\rangle, |V\rangle\}$ or $\{|+\rangle, |-\rangle\}$ and reflect back the encoded photon to Charlie's interrogator to proceed to the measurement step. In addition, an intensity modulator (IM) driven by a quantum random number generator is used to generate decoy states of the pulses to defend against a photon number splitting attack. (See Appendix A for a full description of the security analysis.)

In Figure 2b, the reflected qubits are received to the interrogator, where the BSM in our MDI-QKD implementation protocol can be conveniently performed in the polarization space the same as for the classical MDI-QKD. A successful BSM result corresponds to the observation of precisely two detectors being triggered. From all possible events of separated clicks, the two Bell basis $|\psi^+\rangle$ and $|\psi^-\rangle$ can be deterministically identified:

$$(H,H)or(V,V) \to |\psi^+\rangle, (H,V)or(V,H) \to |\psi^-\rangle \tag{1}$$

3. The Framework for the Key Rate Estimation of MRR-MDI-QKD in a Turbulent Channel

Consider the key rate formula of MDI-QKD [8]

$$R \geq \mu_a\mu_b e^{-(\mu_a+\mu_b)} Y_{11}^{Z}[1 - h(e_{11}^{X}) - Q_{\mu_a\mu_b}^{Z} f(E_{\mu_a\mu_b}^{Z}) h(E_{\mu_a\mu_b}^{Z})] \tag{2}$$

Here, μ denotes the intensity of signal, and $Q_{\mu_a\mu_b}^{Z}$, $E_{\mu_a\mu_b}^{Z}$ are the gain and QBER, respectively, in the Z (signal) basis. $H(x)$ represents the binary Shannon entropy. $Y_{11}^{Z,L}$ is the lower (upper) bound of a single photon yield. $e_{11}^{X,U}$ is the upper bound of the error rate of single photon states, which is estimated from the decoy state statistics in the X basis. Here, $Q_{\mu_a\mu_b}^{Z}$ and $E_{\mu_a\mu_b}^{Z}$ are simulated for rate estimation using known channel transmittance from Alice to Charlie, η_{t_a} (Bob to Charlie, η_{t_b}), respectively, while in experiment they will be measured observables.

To obtain the channel transmittance, we first need to model the free-space channel. Different with a general free-space MDI-QKD, our MRR-MDI-QKD suffers from the double-pass channel, where the total geometric loss in the two passes can be described as [19,20]:

$$\eta_{AC} = \frac{A_{Alice}A_{Charlie}}{\pi\left(\frac{\theta_A}{2}\frac{\theta_C}{2}\right)^2 L_{AC}^4}\exp(-2\beta L_{AC}), \eta_{BC} = \frac{A_{Bob}A_{Charlie}}{\pi\left(\frac{\theta_B}{2}\frac{\theta_C}{2}\right)^2 L_{BC}^4}\exp(-2\beta L_{BC}) \tag{3}$$

Here, $\eta_{AC}(\eta_{BC})$ represents the transmittance of Alice to Charlie (Bob to Charlie) affected by channel loss including atmospheric absorption and geometric spreading loss. $L_{AC}(L_{BC})$ is the distance between Alice (Bob) and Charlie, β is the attenuation coefficient of the free-space link. A_{Alice}, A_{Bob} and $A_{Charlie}$ denote the receiver apertures. θ_A, θ_B and θ_C denote the angle divergences of the transmitter located in Alice, Bob and Charlie, respectively.

Due to the role of the MRR, this process involves the reflection of light. For this, let $I_1(I_2)$ denote the forward-pass (backward-pass) channel coefficient. Taking the average of N samples, they can be formulated as [21]

$$I_1 = \sum_{i=1}^{N} \frac{U_{MMR}^{i} R_{ref}(\theta)}{\sum_{i=1}^{N} U_{in}^{i} circ(D_{tra})} \tag{4}$$

$$I_2 = \sum_{i=1}^{N} U_{out}^{i} circ(D_{tra}) / \sum_{i=1}^{N} U_{MRR}^{i} R_{ref}(\theta) \tag{5}$$

Here, U_{in}^{i}, U_{MRR}^{i} are the amplitudes of the laser beams arriving at Alice (Bob)'s MRR, respectively. U_{out}^{i} is the amplitude of the laser beam received by Charlie, and $circ(D_{MRR})$ is the circular function related with the aperture diameter. Moreover, when the beam diameter $r(\theta)$ is small relative to the aperture, we set $circ(D_{MRR})$ as fixed. In addition, we assumed that $r(\theta)$ is the reflection ratio related with the incident angle with respect to the MRR. Therefore, the reflection effect of the MRR can be written as follows [22]:

$$R_{ref}(\theta) = circ(D_{MRR}) r(\theta) \tag{6}$$

With the above approximations, we now set η_a as total reflection-induced transmission, which can be expressed by

$$\eta_a = RI_1I_2 \tag{7}$$

where the normalized reflection ratio of the MRR R is given by $R_{ref}(\theta)/R_{ref}(0)$.

Furthermore, the optical beam in such a double-pass configuration is jointly affected by the fluctuations of the refractive index (i.e., atmospheric turbulence) in the forward pass from the transceiver to the MRR and that in the backward pass from the MRR to the transceiver, which results in fluctuations in the channel transmittance [23]. To quantify the fluctuations, the Log-normal distribution is considered to characterize the type of weak turbulence conditions. Due to the assumption of uncorrelated fading between the forward and backward passes is not appropriate in the MRR-MDI-QKD configuration, we considered that the double-pass channel can be modeled by the distribution of the weighted product of two correlated Log-normal random variables. Based on the correlated Log-normal distribution with a correlation coefficient ρ_{I}, the probability distribution for the total turbulent-induced fluctuating transmission coefficient [24] is given as:

$$p(\eta_a) = \frac{1}{2\sqrt{2\pi}\eta_a\sigma_{xt}} \exp\left(-\frac{(\ln \eta_a - \ln R - 2\mu_{xt})^2}{8\sigma_{xt}^2}\right) \tag{8}$$

Here, the corresponding μ_{xt} and σ_{xt} are given as:

$$\begin{gathered} \mu_{xt} = \tfrac{1}{2}\ln \mu_1\mu_2 - \tfrac{1}{4}\ln((\tfrac{\sigma_1^2}{\mu_1^2}+1)(\tfrac{\sigma_2^2}{\mu_2^2}+1)), \\ \sigma_{xt} = \sqrt{\tfrac{1}{4}\ln(\tfrac{\sigma_1^2}{\mu_1^2}+1) + \tfrac{1}{4}\ln(\tfrac{\sigma_2^2}{\mu_2^2}+1) + \tfrac{1}{2}\rho_x\sqrt{\ln(\tfrac{\sigma_1^2}{\mu_1^2}+1)\ln(\tfrac{\sigma_2^2}{\mu_2^2}+1)}} \\ \rho_x = 1/\sqrt{\ln(\sigma_1^2/\mu_1^2+1)\ln(\sigma_2^2/\mu_2^2+1)}\,\ln(\rho_I\sigma_1\sigma_2/(\mu_1\mu_2)+1) \end{gathered} \tag{9}$$

Therefore, the total channel transmittance can be respectively defined as:

$$\eta_{t_a} = \eta_a\eta_{AC} \tag{10}$$

To summarize, the secure key rate of our scheme can be obtained as follows:

$$R(\eta) = \int_0^1\int_0^1 p(\eta_{t_a})p(\eta_{t_b})R(\eta_{t_a},\eta_{t_b})d\eta_{t_a}d\eta_{t_b} \tag{11}$$

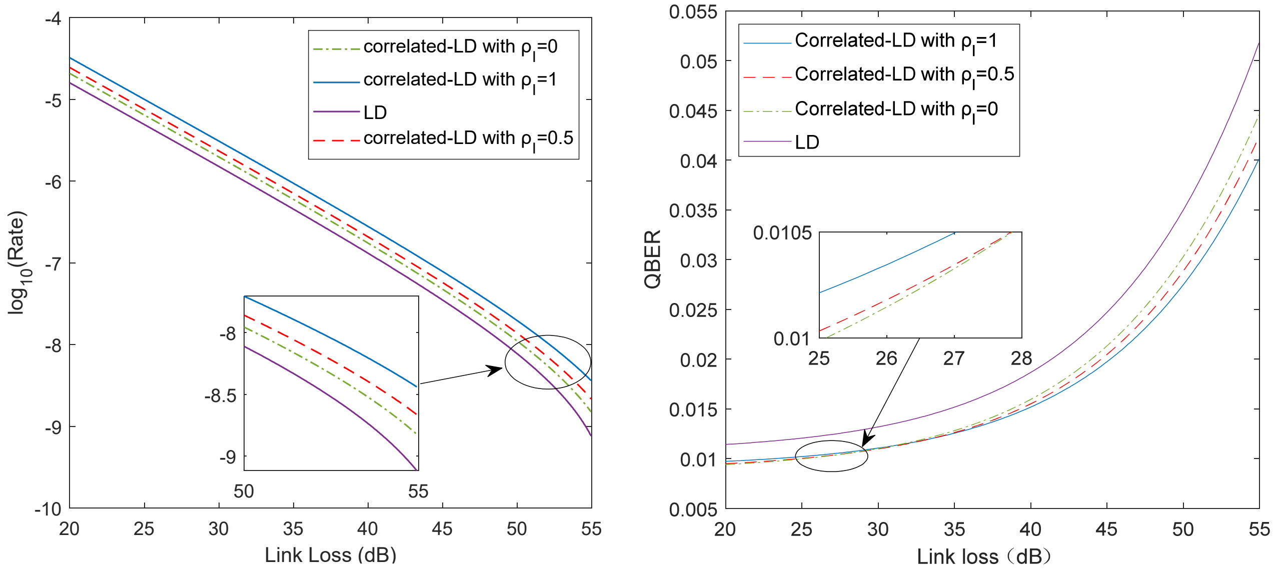
4. Results

In this work, we focus on the symmetric case where the two channel transmissions from Alice to Charlie and from Bob to Charlie are equal. Since we only concentrate on the high-loss region, the geometric loss is ranged from 25 dB~55 dB for convenience. Here, we first compare the key generation rate and QBER using the correlated Log-normal distribution (Correlated-LD) to those using the Log-normal distribution (LD) presented in [24], which are both applicable to the weak turbulence channel. Below for simplicity, we fixed the reflection effect in Equation (6) at 1, which corresponds to the perfect alignment between Alice and Bob. The forward-pass and the backward-pass channel coefficients I_1 and I_2 are also set as 1, respectively. In addition, the signal and decoy state intensity in MDI-QKD setups are fixed at 0.3 and 0.05, respectively. Other numerical parameters are chosen from [25], which are listed in Table 1.

Table 1. Lists of Necessary Parameters.

Symbol	Name	Value
η_{d}	detection efficiency	50%
e_0	error probability of dark counts	0.5
e_d	error probability of optical misalignment	0.015
f_e	error-correction efficiency	1.16
Y_0	background rate	3×10^{-6}

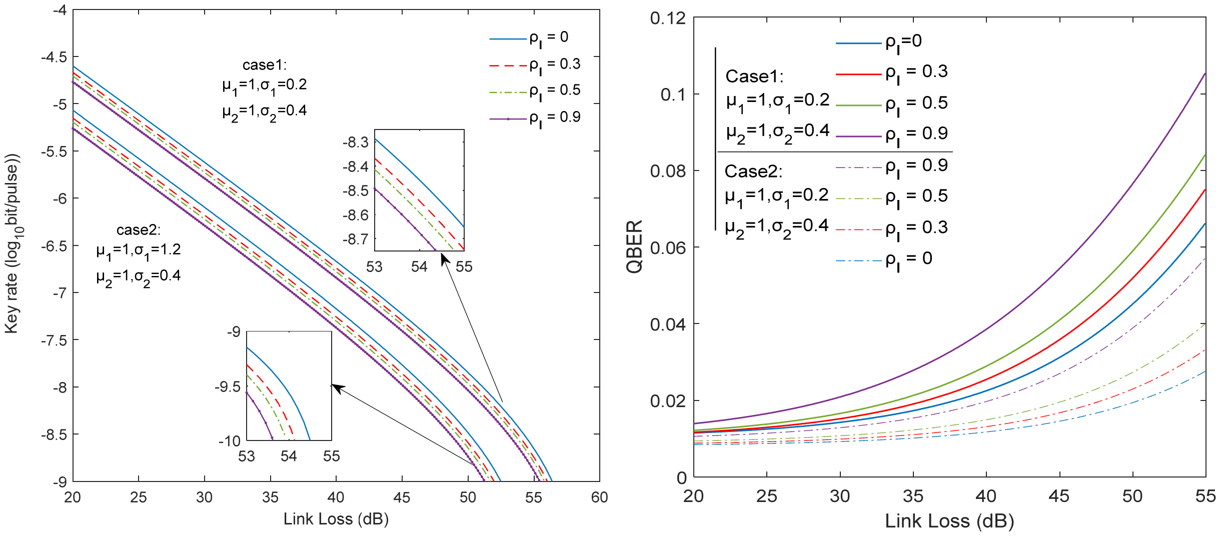
The curves of and the key rate and QBER in the asymptotic case for the two different distributions mentioned above are shown in Figures 3a and 3b, respectively. In Figure 3a, we observe that, in the case with $\rho_{\rm I} = 1$ (i.e., a strict correlation between uplink and downlink), the secret key generation rate in the correlated Log-normal distribution is closer to those in the Log-normal distribution. Furthermore, as shown in Figure 3b, the estimated parameter of QBER clearly shows that the correlated Log-normal distributions are more tightly distributed than the Log-normal distribution, which leads to a higher key rate. The remarkable behavior is that, by scanning through the decoy-state intensities and probabilities, the key rate, in fact, can be further optimized [8,9]. Hence, the correlated Log-normal distributions can give more practical secret key generation estimation.



(**a**) Key rates (**b**) QBER

Figure 3. Key rates and QBER versus channel loss in the two different distributions. For a comparison, the fading correlation coefficient $\rho_{\rm I}$ ranges from 0 to 1, and the turbulence intensity in the forward-pass σ_1 (the backward-pass σ_2) are fixed at 0.3.

We then numerically simulate the performance of our protocol using the correlated Log-normal distributions with different turbulence intensities. The secret key generation rate and QBER in two different weak turbulence cases are show in Figures 4a,b, respectively. For higher channel loss the averaged key rate significantly decreases and the QBER increases. However, we found that there was a slight drop of the key rates, as shown in Figure 4a, when the fading correlation coefficient $\rho_{\rm I}$ increases from 0 to 0.9. Hence, under long-distance propagation distance, the main factor that causes attenuation is still the geometric spreading loss. On the other hand, as shown in Figure 4b, it is a remarkable fact that at a higher channel loss, the QBER in two different turbulence intensity cases grows at different rates, thereby varying degrees of impact on the key rate. This is because the turbulence-induced fluctuating transmittance η_a is related with $E_{uu}(\eta_t)$ and the turbulence intensity σ. Hence the effect of the fading correlation coefficient $\rho_{\rm I}$ on QBER is weak when the channel loss tends to zero and becomes larger with an increase of the product term η_l, which is in agreement with the previous discussion.



(**a**) Key rates (**b**) QBER

Figure 4. Key rates and QBER versus channel loss in the two different weak turbulence cases. The fading correlation coefficient ρ_I ranges from 0 to 0.9. The two different values set for the turbulence intensity σ_1 and σ_2 as {0.4, 0.2} and {0.4, 1.2} were presented in our simulation. When the double-pass channel parameters μ_1, σ_1, μ_2, σ_2 are fixed, the performance is impaired by the fading correlation coefficient ρ_{I} and deteriorating with increasing ρ_{I}. When the fading correlation coefficient ρ_{I} is fixed, the key rates of our scheme increase with the decrease of the turbulence intensity σ_2 .

5. Conclusions

In this paper, a modified MDI-QKD scheme with modulating retro-reflectors is proposed not only to inherit the merit of the structure in which the experimental system is automatically stabilized in spectrum and polarization modes, but also to bring advantages of the MRR that simplify the pointing requirements due to its wide reflective field of view. Here, the double-pass correlated turbulent channel model is used to investigate the complex and unstable channel characteristics caused by the atmospheric turbulence. The simulation results clearly show that the correlated Log-normal distribution is more appropriate to characterize the correlated fading in the MRR-MDI-QKD, which could be used as a modeling method when estimating secret key rate in such free-space QKD configuration. Moreover, inspired by the idea of the Plug-and-Play MDI-QKD, the security analysis of MRR-MDI-QKD is analyzed under some classical attacks, which ensures that the MRR-MDI-QKD can be implemented with only ordinary optical elements in the experiment. Our work provides a meaningful step towards an MDI-QKD based on the moving platforms to join a dynamic quantum network with untrusted relays.

Author Contributions: Conceptualization, X.W. and W.L.; methodology, X.W.; software, T.W.; validation, X.W. and W.L. and T.W.; formal analysis, X.W.; investigation, Y.Z., X.W.; resources, X.W.; data curation, C.G.; writing—original draft preparation, X.W.; writing—review and editing, W.L. and C.G.; visualization, T.W.; supervision, T.W.; project administration, S.Z.; funding acquisition, S.Z. and C.D. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the National Natural Science Foundation of China under Grant No. 61971436, in part by the National University of Defense Technology under Grant No. 19-QNCXJ, in part by the Innovative Talents Promotion Plan in Shaanxi Province under Grant No. 2020KJXX-011, in part by the Key Research and Development Program of Shaanxi under Grant No. 2019ZDLGY09-01, in part by the Innovative Key Projects Promotion in Information and Communication College (No. YJKT-ZD-2105), and in part by the Innovative Talents Promotion in Information and Communication College (No. YJKT-RC-2113).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data is contained within the article.

Acknowledgments: We thank Wenyuan Gu for helpful discussions.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A. Security Analysis

The MRR-MDI-QKD links share the same characteristics of general plug-and-play QKD links, and as a result also were faced with similar security issues. In this section, we give priority to consider the security implications of untrusted light sources caused by the structure. A complete proof of the unconditional security of MDI-QKD with an untrusted source is derived in [2], which considered various real-life imperfections in its implementation. Moreover, a general formalism is proposed to prove the security of MDI-QKD with leaky sources to relax this unrealistic assumption [26]. Specifically, there is no information leakage from the transmitters to the senders, which shows that MDI-QKD is feasible within a reasonable time frame of signal transmission given that the sources are sufficiently isolated. Reference [27] demonstrated a proof-of-principle experiment over an asymmetric 36 km fiber channel to improve the feasibility of plug-and-play MDI-QKD and discuss the methods to improve security by increasing active monitoring.

In practice, Bob limits his interrogation power and Alice adjusts the double pass loss of the MRR array to change the mean number of photons that are retro-reflected to implement the decoy state method, which is usually used to defend against photon number splitting attacks. The intercept-resend attacks can be defeated with active countermeasures, where Alice also uses the photo detection capability to monitor the incoming power of all four MRRs. The Trojan horse attack, which is the main threat in plug and play systems, can be effectively defended by increasing active monitoring to detect the incoming optical power. Though our modified plug-and-play MDI-QKD scheme with MRR is vulnerable to the source attacks also facing in plug-and-play QKD schemes, the unique characteristics of the MRR devices allow them to act as both power and angle of arrival detectors without adding extra components to the system.

References

1. Lo, H.K.; Curty, M.; Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **2012**, *108*, 130503. [CrossRef] [PubMed]
2. Braunstein, S.L.; Pirandola, S. Side-Channel-Free Quantum Key Distribution. *Phys. Rev. Lett.* **2012**, *108*, 130502. [CrossRef] [PubMed]
3. Rubenok, A.; Slater, J.A.; Chan, P.; Lucio-Martinez, I.; Tittel, W. Real-World Two-Photon Interference and Proof-of-Principle Quantum Key Distribution Immune to Detector Attacks. *Phys. Rev. Lett.* **2013**, *111*, 130501. [CrossRef] [PubMed]
4. Wang, X.-B. Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography. *Phys. Rev. Lett.* **2005**, *94*, 230503. [CrossRef]
5. Da Silva, T.F.; Vitoreti, D.; Xavier, G.; Amaral, G.; Temporão, G.P.; Von Der Weid, J.P. Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits. *Phys. Rev. A* **2013**, *88*, 052303. [CrossRef]
6. Liu, Y.; Chen, T.-Y.; Wang, L.-J.; Liang, H.; Shentu, G.-L.; Wang, J.; Cui, K.; Yin, H.-L.; Liu, N.-L.; Li, L.; et al. Experimental Measurement-Device-Independent Quantum Key Distribution. *Phys. Rev. Lett.* **2013**, *111*, 130502. [CrossRef]
7. Yin, H.-L.; Chen, T.-Y.; Yu, Z.-W.; Liu, H.; You, L.; Zhou, Y.-H.; Chen, S.-J.; Mao, Y.; Huang, M.-Q.; Zhang, W.-J.; et al. Measurement-Device-Independent Quantum Key Distribution Over a 404 km Optical Fiber. *Phys. Rev. Lett.* **2016**, *117*, 190501. [CrossRef]
8. Wang, X.-B. Three-intensity decoy-state method for device-independent quantum key distribution with basis-dependent errors. *Phys. Rev. A* **2013**, *87*, 012320. [CrossRef]
9. Zhou, Y.-H.; Yu, Z.-W.; Wang, X.-B. Making the decoy-state measurement-device-independent quantum key distribution practically useful. *Phys. Rev. A* **2016**, *93*, 042324. [CrossRef]
10. Pirandola, S.; Andersen, U.L.; Banchi, L.; Berta, M.; Bunandar, D.; Colbeck, R.; Wallden, P. Advances in quantum cryptography. *Adv. Opt. Photonics* **2020**, *12*, 1012–1236. [CrossRef]
11. Cao, Y.; Li, Y.-H.; Yang, K.-X.; Jiang, Y.-F.; Li, S.-L.; Hu, X.-L.; Abulizi, M.; Li, C.-L.; Zhang, W.; Sun, Q.-C.; et al. Long-Distance Free-Space Measurement-Device-Independent Quantum Key Distribution. *Phys. Rev. Lett.* **2020**, *125*, 260503. [CrossRef]
12. Wang, X.; Dong, C.; Zhao, S.; Liu, Y.; Liu, X.; Zhu, H. Feasibility of space-based measurement-device-independent quantum key distribution. *New, J. Phys.* **2021**, *23*, 045001. [CrossRef]
13. Tarantino, S.; Da Lio, B.; Cozzolino, D.; Bacco, D. Feasibility study of Quantum Communications in Aquatic Scenarios. *Optik* **2020**, *216*, 164639. [CrossRef]

14. Chen, Y.-A.; Zhang, Q.; Chen, T.-Y.; Cai, W.-Q.; Liao, S.-K.; Zhang, J.; Chen, K.; Yin, J.; Ren, J.-G.; Chen, Z.; et al. An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature* **2021**, *589*, 214–219. [CrossRef]
15. Born, B.; Hristovski, I.R.; Geoffroy-Gagnon, S.; Holzman, J.F. All-optical retro-modulation for free-space optical communication. *Opt. Express* **2018**, *26*, 5031–5042. [CrossRef]
16. Rabinovich, W.S.; Mahon, R.; Ferraro, M.S.; Goetz, P.G.; Bashkansky, M.; Freeman, R.E.; Reintjes, J.; Murphy, J.L. Free space quantum key distribution using modulating retro-reflectors. *Opt. Express* **2018**, *26*, 11331–11351. [CrossRef] [PubMed]
17. Yang, G.W.; Li, C.; Li, Y.J.; Geng, H.J.; Bi, M.H.; Fan, B.; Wang, T.S. Channel Modeling and performance analysis of modulating retro reflector FSO systems under weak turbulence conditions. *IEEE Photonics J.* **2017**, *9*, 1–10.
18. Choi, Y.; Kwon, O.; Woo, M.; Oh, K.; Han, S.-W.; Kim, Y.-S.; Moon, S. Plug-and-play measurement-device-independent quantum key distribution. *Phys. Rev. A* **2016**, *93*, 032319. [CrossRef]
19. Trinh, P.V.; Pham, T.V.; Nguyen, H.V.; Ng, S.X.; Pham, A. Performance of Free-Space QKD Systems Using SIM/BPSK and Dual-Threshold/Direct-Detection. In Proceedings of the 2016 IEEE Globecom Workshops, Washington, DC, USA, 4–8 December 2016; pp. 1–6. [CrossRef]
20. Trinh, P.V.; Pham, A.; Dang, N.T.; Nguyen, H.; Ng, S.X.; Phama, A.T. Design and Security Analysis of Quantum Key Distribution Protocol Over Free-Space Optics Using Dual-Threshold Direct-Detection Receiver. *IEEE Access* **2018**, *6*, 4159–4175. [CrossRef]
21. Abadi, M.M.; Ghassemlooy, Z.; Zvanovec, S.; Bhatnagar, M.R.; Khalighi, M.A.; Wu, Y. Impact of link parameters and channel correlation on the performance of FSO systems with the differential signaling technique. *IEEE J. Opt. Commun. Netw.* **2017**, *9*, 138–148. [CrossRef]
22. Minott, P.O. *Design of Retrodirector Arrays for Laser Ranging of Satellite*; NASA TM-X-723-74-122; goddard Space Flight Center: Greenbelt, MD, USA, 1974; pp. 1–21.
23. You, S.; Yang, G.; Bi, M.; Wei, Y.; Lu, Y.; Zhou, X. Wave-optics simulation of the channel fading in modulating retro-reflector free-space optical link. In Proceedings of the 2015 International Conference on Wireless Communications & Signal Processing (WCSP), Nanjing, China, 15–17 October 2015; pp. 1–5. [CrossRef]
24. Zhu, Z.-D.; Chen, D.; Zhao, S.-H.; Zhang, Q.-H.; Xi, J.-H. Real-time selection for free-space measurement device independent quantum key distribution. *Quantum Inf. Process.* **2018**, *18*, 33. [CrossRef]
25. Tang, G.-Z.; Sun, S.-H.; Xu, F.; Chen, H.; Li, C.-Y.; Liang, L.-M. Experimental asymmetric plug-and-play measurement-device-independent quantum key distribution. *Phys. Rev. A* **2016**, *94*, 032326. [CrossRef]
26. Wang, W.; Tamaki, K.; Curty, M. Measurement-device-independent quantum key distribution with leaky sources. *Sci. Rep.* **2021**, *11*, 1–11. [CrossRef]
27. Liao, Q.; Wang, Y.; Huang, D.; Guo, Y. Dual-phase-modulated plug-and-play measurement-device-independent continuous-variable quantum key distribution. *Opt. Express* **2018**, *26*, 19907–19920. [CrossRef] [PubMed]