Dynamic attenuation scheme in measurement-device-independent quantum key distribution over turbulent channels

Brian J. Rollick[*] and George Siopsis[‡]
Department of Physics and Astronomy, University of Tennessee, Knoxville, Tennessee 37996-1200, USA

Bing Qi[†]
Cisco Systems, San Jose, California 95134, USA

(Received 25 April 2022; accepted 15 August 2022; published 2 September 2022)

Measurement-device-independent quantum key distribution (MDI QKD) offers great security in practice because it removes all detector side channels. However, conducting MDI QKD over free-space channels is challenging. One of the largest culprits is the mismatched transmittance of the two independent turbulent channels causing a reduced Hong-Ou-Mandel visibility and thus a lower secret key rate. Here we introduce a dynamic attenuation scheme, where the transmittance of each of the two channels is monitored in real time by transmitting bright light pulses from each users to the measurement device. Based on the measured channel transmittance, a suitable amount of attenuation is introduced to the low-loss channel at the measurement device. Our simulation results show a significant improvement of QKD performance, especially when using short raw keys.

DOI: 10.1103/PhysRevA.106.032405

I. INTRODUCTION

Ever since the Bennett-Brassard 1984 (BB84) protocol was proposed, quantum key distribution (QKD) has enjoyed tremendous progress. In particular, free-space experiments have progressed from just 30-cm [1] to 7600-km satellite-based connections [2].

Despite this progress, numerous hacking techniques have been discovered. While in theory, QKD is secure, realistic implementations deviate from ideal models used in the security proofs. In particular, detectors may be vulnerable to a plethora of attacks, including the detector blinding attack [3,4], time-shift attack [5], backflash attack [6], and many others (see Jain *et al.* [7]).

Two types of countermeasures have been proposed. The first type involves addressing new attacks as they are discovered and adjusting the setup accordingly in order to thwart them. An example of such countermeasures is adding an optical isolator to combat the backflash attack. However, unknown attacks cannot be anticipated. The second type involves device-independent QKD (DI QKD) protocols [8–10]. In this category, a common entanglement source sends photon pairs to Alice and Bob. Because entanglement is monogamous, the protocol is provably secure with the proof relying directly on the violation of Bell's inequalities [11]. However, a loophole-free Bell test is very challenging in practice [12]. For a recent experimental demonstration of DI-QKD, see Ref. [13].

A more practical protocol, called measurement-device-independent QKD (MDI QKD) [14], automatically removes all detector side-channels by employing time-reversed entanglement. In this protocol, Alice and Bob send light pulses to a third party, Charlie, who possesses a Bell-state analyzer based on linear optics and single-photon detection. Charlie projects the input photons to Bell states and publicly announces the measurement results, which allows Alice and Bob to generate a secret key by classical postprocessing. MDI QKD has been widely implemented with attenuated laser sources that incorporate the decoy-state protocol [15–17]. It has also been implemented on chips [18] and with cost-effective setups [19].

The Bell-state analyzer in MDI QKD relies on the Hong-Ou-Mandel (HOM) effect [20] where photons from Alice and Bob interfere at a 50:50 beam splitter. A high HOM visibility can usually be translated into a low quantum bit error rate (QBER) and therefore a high secret key rate. To achieve a high HOM visibility, photons from Alice and Bob should be indistinguishable in all degrees of freedom. Furthermore, when the MDI QKD is implemented with weak coherent sources, a high HOM visibility requires the average photon numbers from Alice and Bob to be matched at the beam splitter [21,22].

In practice, the two quantum channels (one from Alice to Charlie, and another from Bob to Charlie) may have different transmittance. One could account for this mismatch by simply adding extra fiber on the low-loss channel so that each channel equally attenuates the light pulses [15]. While being unwieldy in a future quantum network with many users, this approach can improve the HOM visibility at the cost of a lower detection rate. A better solution is the asymmetric MDI QKD protocol where Alice and Bob use different intensity profiles [23,24]. The asymmetric MDI QKD allows Alice and Bob to send different intensities to help account for the asymmetric

[*]brollick@vols.utk.edu
[†]bingq@cisco.com
[‡]siopsis@tennessee.edu

channel loss. This results in a large improvement over simply adding fiber [24].

Unfortunately, the above asymmetric MDI QKD protocol requires static channels (such as optical fiber) and may not be applicable in free-space MDI QKD, where the transmittance of each of the two channels fluctuates randomly and independently of the other channel. Asymmetric protocols could still help for compensating the mismatch of the average channel losses. To compensate for the channel fluctuation, Alice and Bob would have to know the instantaneous channel transmittance and change their QKD parameters on the scale of milliseconds [25].

In free-space BB84 setups, an adaptive postselection scheme was proposed where a stronger probe beam would be multiplexed with the single-photon pulses to monitor the atmospheric transmittance at a given time [26–29]. The time blocks with lower transmittance would correspond to a higher QBER. Hence, discarding pulses measured in those blocks could increase the key rate despite reducing the detection rate [30]. Recent work, such as Refs. [31–33], has also introduced this idea to MDI QKD.

In this work, we propose a dynamic attenuation scheme to improve the key rate of free-space MDI QKD. Similar to the adaptive postselection scheme in BB84 QKD, both Alice and Bob transmit strong probe beams with known intensities to Charlie, who determines the channel transmittances in real time by measuring probe beams with classical photodetectors and then applies an appropriate amount of attenuation on one of the paths to compensate for the mismatch of channel transmittance. The effect is similar to the case of adding extra fiber in asymmetric channels. Our simulations show that using dynamic attenuation makes MDI QKD considerably more robust in turbulence. In the high-turbulence region, our scheme still shows improvement even when we consider a nonzero minimum loss for Charlie's variable attenuators.

Our discussion is organized as follows. Section II contains pertinent background for MDI QKD, discusses how turbulence affects transmission, and details our proposed scheme. Section III outlines our simulation model and presents our results. Lastly, Sec. V contains a brief discussion of our approach and suggests future work. Details of the noise model we used and the secure key calculation are provided in the Appendix.

II. THEORY

A. Polarization encoding MDI QKD

Inspired by time-reversed entanglement [34,35], MDI QKD was proposed as a solution to detector side-channel attacks. In this protocol, Alice and Bob generate a key by sending laser pulses to a potentially untrusted third party, Charlie, who projects them onto Bell states and publicly announces his results. In general, they may choose time-bin encoding [36–38], phase encoding [39], or polarization encoding [16,40]. Here, we work with polarization encoding.

Phase-randomized weak coherent pulses remain common in QKD implementations. To improve the performance of QKD, decoy-state protocols are employed [41–43]. The original MDI QKD protocol used three different intensities

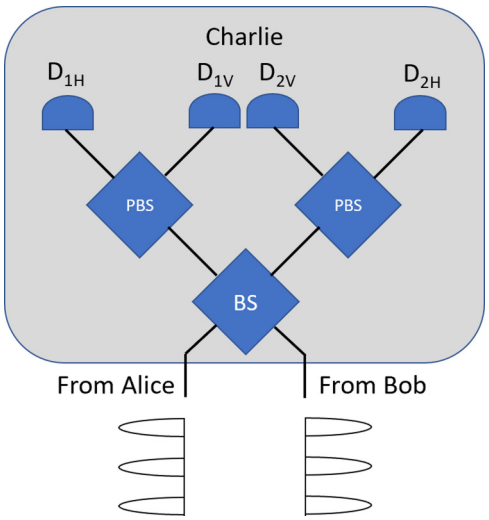

FIG. 1. Basic measurement setup for Charlie in a polarization encoding MDI QKD experiment. Alice and Bob send pulsed laser beams to Charlie whose experimental setup consists of a beam splitter (BS), two polarization beam splitters (PBS), and four single-photon detectors (D). Charlie publicly announces his measurement results and one of Alice and Bob may apply bit-flip depending on the Bell state detected and the encoding basis.

[14,44]. Zhou *et al.* then showed a sizable improvement with a four-intensity method [45]. A seven-intensity method was also suggested to account for asymmetric channels in Ref. [24] where Alice and Bob could choose their signal and decoy parameters independently to account for asymmetric loss. In this work, we only consider channels with identical statistical distribution, so the four-intensity protocol is adopted.

In MDI QKD with polarization encoding, Alice and Bob encode their random bits on the polarization of weak coherent states, using one of the two bases, rectilinear (Z) or diagonal (X), and Charlie performs Bell-state measurements using a setup depicted in Fig. 1.

A bit of raw key is generated whenever Charlie measures a coincidence of photons with orthogonal polarizations (V and H, respectively) using a set of four single-photon detectors, $\{D_{1H}, D_{1V}, D_{2H}, D_{2V}\}$, and Alice and Bob use the same encoding basis. Charlie announces the outcome $|\psi^-\rangle$ whenever coincidences occur on $D_{1V}D_{2H}$ or $D_{1H}D_{2V}$, and he announces $|\psi^+\rangle$ if coincidences occur on $D_{1H}D_{1V}$ or $D_{2H}D_{2V}$, instead. Other detection patterns are simply discarded. In the rectilinear basis, errors occur whenever Alice and Bob send the same polarization, and Charlie announces $|\psi^-\rangle$ or $|\psi^+\rangle$. In the diagonal basis, errors occur whenever Alice and Bob send the same polarization and Charlie announces $|\psi^-\rangle$ or Alice and Bob send orthogonal polarization states and Charlie announces $|\psi^+\rangle$.

Notice in Fig. 1 that Charlie only measures in the rectilinear basis. To ensure a low error rate when Alice and Bob use the diagonal basis, Charlie relies on the HOM effect to bunch identical photons from Alice and Bob at the beam splitter. High HOM visibility requires Alice's and Bob's photons to be identical in every degree of freedom at the beam splitter. In the case of phase-randomized weak coherent sources, the average photon numbers from Alice and Bob should be matched at

the beam splitter [21,22]. Consequently, it can be difficult to consistently achieve high HOM visibility in a turbulent atmosphere with fluctuating transmittance. The central idea of our dynamic attenuation scheme is to compensate the transmittance mismatch by dynamically controlling the amount of attenuation introduced.

B. Atmospheric effects

The transmittance coefficient of light η follows a lognormal distribution through a weak to moderate turbulent channel [46–48]. In this regime, we can express the effect of turbulence using two parameters, the average transmittance η_0 and the log irradiance variance σ^2 which characterizes the severity of the turbulence. The probability distribution of the transmittance coefficient (PDTC) is given by

$$P(\eta) = \frac{1}{\sqrt{2\pi}\sigma\eta} e^{\frac{-\left[\ln\left(\frac{\eta}{\eta_0}\right)+\frac{\sigma^2}{2}\right]^2}{2\sigma^2}}. \tag{1}$$

Very weak to moderately strong turbulence for a 3-km channel has σ^2 ranging from 10^{-3} to about 1.2 at 1550-nm wavelength. After this point, the lognormal distribution for transmittance loses validity [46].

The average loss η_0 can be determined from atmospheric visibility and channel length. Due to the complexity of different atmospheric and aerosol models, software such as MODTRAN [49,50] and FASCODE [51] is often required to find transmittance for an arbitrary wavelength.

In this work, we consider average losses of $\eta_0 = 17$, 14, 11, and 8 dB in each channel (excluding the efficiency of detector), and we choose QKD parameters based on a recent free-space MDI-QKD demonstration [31]. We then simulate the secret key rate using a range of values for σ^2 and show that dynamic attenuation makes MDI QKD more tolerant of channel fluctuation.

C. Dynamic attenuation scheme

We propose a scheme where high-speed, low-loss variable optical attenuators (VOAs) are placed before Charlie's beam splitter (see Fig. 2) to balance the transmittance fluctuations between the two channels. Both Alice and Bob transmit strong probe beams with known intensities along the same paths as the QKD signals, but slightly separated in wavelength. Charlie can separate the probe beams from the QKD signals using dense wavelength-division multiplexing (DWDM) technology and determine the channel transmittance in real time by measuring probe beams with classical photodetectors. He further applies an appropriate amount of attenuation on the high-transmittance path.

The goal of adding additional attenuation is to balance the loss between the two channels and improve the HOM visibility. However, because additional loss could negatively impact the raw key rate, an optimal balance must be found to maximize the final secret key rate, as we discuss below.

If we assume Alice's and Bob's channels are independent, the joint probability distribution is simply

$$P(\eta_A, \eta_B) = P(\eta_A)P(\eta_B), \tag{2}$$

where $P(\eta)$ is defined in Eq. (1).

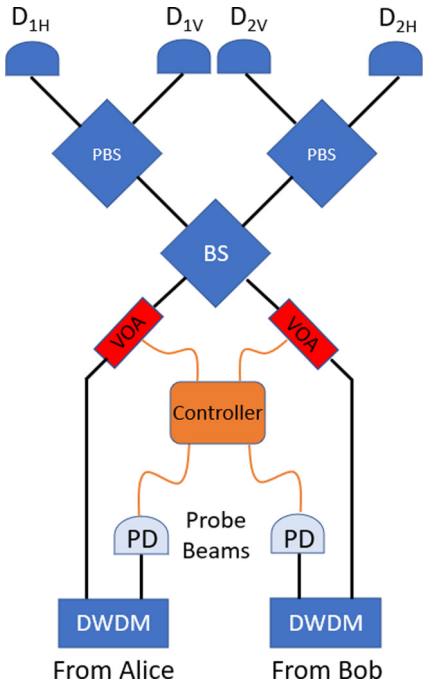

FIG. 2. Charlie's measurement setup with dynamic attenuation using probe beams sent by Alice and Bob. The multiplexed probes are separated by DWDMs and their intensities are measured using classical light detectors. Charlie, based on the measurement results of the probe beams, applies a proper amount of attenuation to the channel with lower loss using variable optical attenuators.

Since the secret key rate is a function of transmittance, one can compute the average key rate using the following integral, given an infinite key length:

$$R_{\text{ave}} = \int_0^1 \int_0^1 R(\eta_A, \eta_B)P(\eta_A)P(\eta_B)d\eta_A d\eta_B, \tag{3}$$

where we used Eq. (2) for the joint probability distribution. $R(\eta_A, \eta_B)$ is the key rate bounded by [14]

$$R \geqslant P_Z^{1,1}Y_Z^{1,1}\left[1 - H_2\left(e_X^{1,1}\right)\right] - Q_Z f_{\text{EC}}(E_Z)H_2(E_Z), \tag{4}$$

where $P_Z^{1,1}$ is the probability of sending a single-photon pair in the Z basis, $Y_Z^{1,1}$ is the yield of a single-photon pair in the Z basis, and Q_Z and E_Z are the gain and error rates, respectively. $e_X^{1,1}$ is the error rate of a single photon in the X basis, f_{EC} is the error-correcting efficiency, and $H_2(x)$ is the Shannon binary entropy function.

When using dynamic attenuation, the joint PDTC is transformed according to

$$P(\eta_A\prime, \eta_B\prime) = \iint K(\eta_A\prime, \eta_B\prime, \eta_A, \eta_B)P(\eta_A, \eta_B)d\eta_A d\eta_B, \tag{5}$$

where $K(\eta_A\prime, \eta_B\prime, \eta_A, \eta_B)$ represents the kernel relating the new joint PDTC with the original one. Because we cannot achieve infinite resolution, a lookup table is used instead of the kernel.

If we use the lookup table to transform the joint probability distribution, the asymptotic key rate after dynamic attenuation

TABLE I. η_D is the detector efficiency, e_{dZ} and e_{dX} are misalignments in their respective bases, Y_0 is the dark count probability, and f_{EC} is the error-correction efficiency.

η_D	e_{dZ}	e_{dX}	f_{EC}	Y_0
0.5	0.003	0.03	1.1	7×10^{-7}

is found from Eq. (3). We deduce

$$R'_{\mathrm{ave}} = \int_0^1 \int_0^1 R(\eta_{A'}, \eta_{B'}) P(\eta_{A'}, \eta_{B'}) d\eta_{A'} d\eta_{B'}, \tag{6}$$

where the integral is evaluated numerically.

Furthermore, Eq. (6) must be modified in the case of finite key size, because when additional loss is introduced, the finite size effect is exacerbated. Consequently, rather than integrate the PDTC against the secure key rate, we integrate to find new sifted key and error sizes $\{n_Z, n_X, m_Z, m_X\}$ and use a bounded version of Eq. (4) afterward. Thus, we separately compute the following:

$$n^{i,j}_{X,Z} = \int_0^1 \int_0^1 n^{i,j}_{X,Z}(\eta_A, \eta_B) P(\eta_{A'}, \eta_{B'}) d\eta_{A'} d\eta_{B'}, \tag{7}$$

$$m^{i,j}_{X,Z} = \int_0^1 \int_0^1 m^{i,j}_{X,Z}(\eta_A, \eta_B) P(\eta_{A'}, \eta_{B'}) d\eta_{A'} d\eta_{B'}, \tag{8}$$

where $n^{i,j}_{X,Z}$ and $m^{i,j}_{X,Z}$ represent the number of sifted bits and errors, respectively, in the X and Z bases and for i and j states (signal, or one of the decoy states) from Alice and Bob. Once the sifted bits and errors have been found, we compute the full secure key length using our sifted bits and errors and QKD system parameters. A detailed description of the key calculation can be found in the Appendix.

III. PARAMETER OPTIMIZATION AND KERNEL GENERATION

In QKD using decoy states [41–43], it is essential to optimize the intensity of each state and the probability of sending it. Here, we employ the four-intensity protocol; therefore, six parameters must be optimized. In particular, Alice and Bob use the set of intensities $\{s, \mu, \nu, \omega\}$, where s is the signal state intensity, μ and ν are the decoy state intensities, and $\omega = 0$ is the vacuum state.

We optimize decoy parameters stochastically using MATLAB's built-in genetic algorithm. This is a preferred technique because it requires neither differentiability nor any initial data points. It also runs reasonably quickly on an ultrabook's Ryzen 5 processor.

Prior to optimization, we choose the total number of pulses N, Z-basis misalignment e_{dZ}, X-basis misalignment e_{dX}, dark counts Y_0, detector efficiencies η_D, and an estimated channel transmittance η_0. Our choices are taken from a recent free-space MDI-QKD experiment in Ref. [31] and are listed in Table I.

Because the lognormal distribution's median is considerably less than the mean for higher turbulence, about 3–6 dB of extra loss in each arm must be budgeted into η_0 at the optimization and lookup stages, compared to the simulation step. We, therefore, optimize channels assuming $\eta_0 \in \{0.01, 0.02, 0.04\}$.

In the optimization and lookup table generation, we compute the finite secure key rate using

$$R = P_s^2 \left\{ s^2 e^{-2s} Y^{1,1}_{X,\min} \left[1 - H_2\left(e^{1,1,\max}_X \right) \right] - Q_Z f_{\mathrm{EC}}(E_Z) H_2(E_Z) \right\}, \tag{9}$$

where P_s is the probability of sending a signal state, s is the average photon number of the signal state, $Y^{1,1}_{X,\min}$ is the lower bound of a single-photon pair yield in the X basis, and Q_Z and E_Z are the Z-basis (signal) gain and error rates, respectively. $e^{1,1}_{X,\max}$ is the upper bound of the single-photon pair error rate in the X basis, f_{EC} is the error-correcting efficiency, and $H_2(x)$ is the Shannon binary entropy function. A detailed calculation can be found in the Appendix.

Once decoy parameters are obtained, the lookup table is generated where the transmittance of Alice's and Bob's channels are varied in the range $0.001 \leqslant \eta_0 \leqslant 1$ in increments of about 0.001. For each pair of transmittances, we compute the key rate using Eq. (9) assuming a static channel. Specifically, we evaluate the key rate after applying an additional 0.1 dB to the stronger channel until we find the maximum.

The case in Fig. 3 represents the procedure needed to produce a single point in the final lookup table. In this example, we select transmittances of $\eta_A = 0.15$ and $\eta_B = 0.04$ and we apply an incremental attenuation of 0.1 dB to Alice's side to bring hers closer to Bob's. Each point represents 0.1 dB of additional attenuation for Alice since her channel has higher transmittance. Figure 3(a) shows the improvement in secure key rate as we attenuate Alice's (stronger) side. Notice in Fig. 3(b), as we attenuate Alice, we see improved HOM visibility at the expense of single-photon yield. We balance these two effects by evaluating Eq. (9) for each point, where we assume an entire experiment with data size N was conducted with new transmittance, t_A. We observe the maximum improvement to the key rate at about 2 dB of attenuation, which we record in the lookup table for these two transmittances.

A plot of the optimal attenuation as a function of transmittance of Alice's and Bob's channels is shown in Fig. 4. Here, we observe that the optimum is zero additional attenuation for many combinations of transmittances, except when their imbalance is large. However, the channels will most likely be highly imbalanced when the atmospheric turbulence is strong. If we apply the optimal attenuation, the impact on the secret key rate, as shown in Fig. 5, increases precipitously as the imbalance goes up. The reason is because for much of the yellow region the key rate without dynamic attenuation vanishes rapidly for higher mismatch.

Computing time determines the fineness of the lookup table. The finer the resolution, the more accurately the table will approximate the ideal kernel K [Eq. (5)]. Improvements can still be seen when the resolution is more coarse than about 0.001, but the effects are less pronounced.

IV. RESULTS

Once the lookup table is produced for a given set of parameters, we produce PDTCs for different atmospheric conditions using Eq. (1). We start with very weak turbulence of $\sigma^2 = 0.001$ and go up to $\sigma^2 = 1.2$, after which we would need to

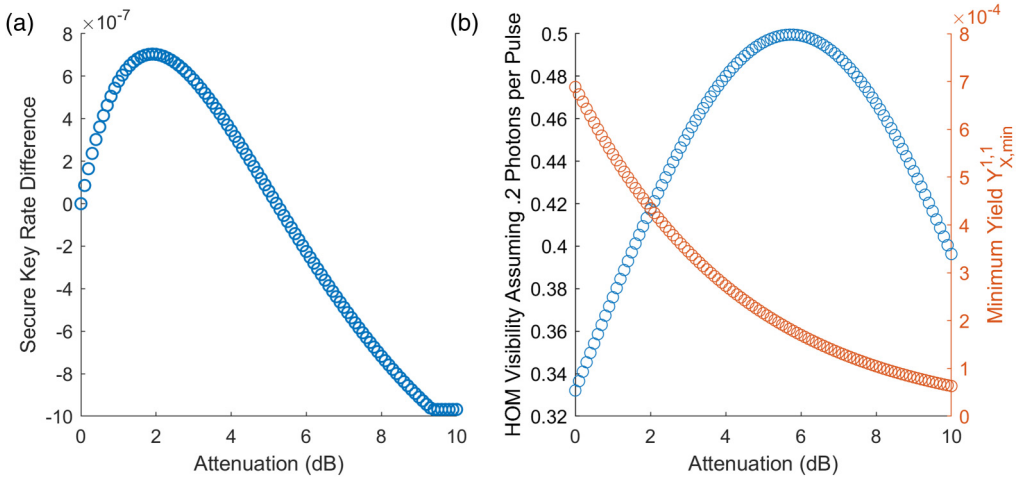

FIG. 3. Results using a lookup table for $\eta_A = 0.15$, $\eta_B = 0.04$, and $N = 10^{13}$ pulses. (a) Improvement in secure key rate when we attenuate the stronger channel (Alice). (b) Improvement of the HOM visibility, thereby our estimate of $e_X^{1,1}$, and the decrease in yield as Alice's channel is attenuated.

move beyond the lognormal model of turbulence [46]. Our choices of η_0 assume losses of 17, 14, 11, and 8 dB in each channel.

To produce each PDTC, we numerically integrate to determine the number of sifted bits for each pair of transmittances, as in Eq. (8). The integral is computed by evaluating the PDTCs in 0.001 increments in the range $0 \leqslant \eta \leqslant 1$, for both Alice's and Bob's channels, and finding the number of sifted bits contributing to the final key. We evaluate the noise model using each pair of transmittances, additionally attenuate the stronger transmittance using the lookup table, and separately determine the number of sifted bits and errors for both cases.

Afterward, we evaluate the secure key rate corresponding to the sifted bit and error sizes for the original PDTC and the transformed PDTC. Results are shown in Fig. 6, and decoy parameters for each run are given in Table II.

In Fig. 6 we see the greatest impact when working at the strongest amounts of turbulence (indicated by increasing σ) and thus channel imbalance. In particular, for many of the plots shown, we see that dynamic attenuation gives the ability to generate a secure key when the atmospheric conditions would not otherwise allow it.

Results show that dynamic attenuation gives a higher secure key rate when the turbulence-induced transmittance fluctuation is more severe, as manifested by a higher σ^2. The

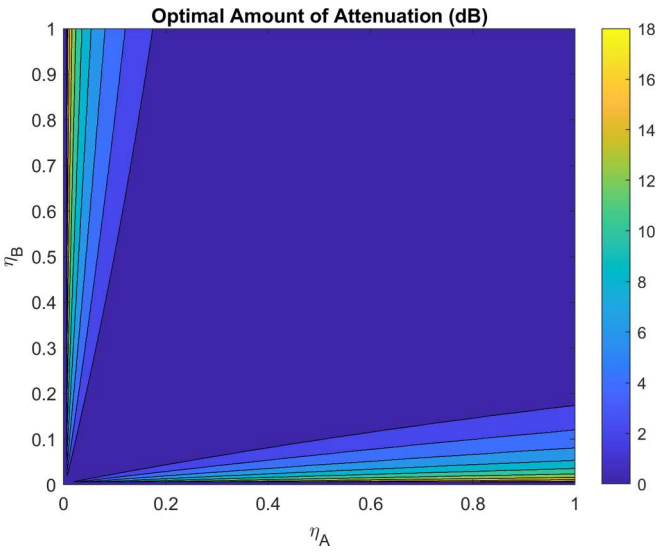

FIG. 4. Plot of the optimal amount of attenuation needed to produce the highest key rate for different combinations of Alice's and Bob's transmittances when $N = 10^{14}$. The middle of the plot requires no additional attenuation because the transmittances are already close. In high turbulence, Alice's and Bob's channels will likely have very different transmittances and hence dynamic attenuation is useful to enhance the key rate.

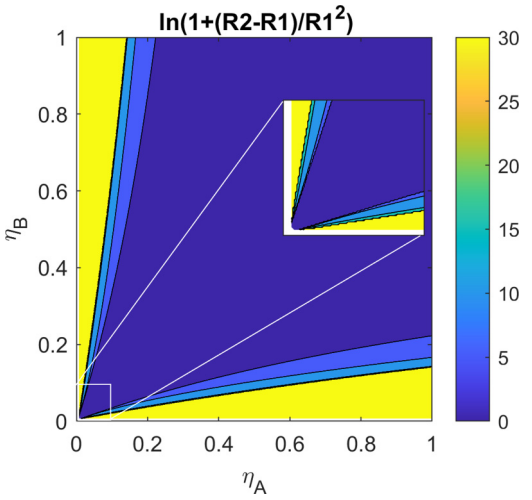

FIG. 5. Improvement in the secure key rate when the optimal attenuation is applied, where $R2$ and $R1$ are the key rates with and without dynamic attenuation. Under turbulent conditions, when Alice's and Bob's transmittances fluctuate the most, and transmittances are likely very different, Alice and Bob see the greatest benefit of dynamic attenuation. In the white region near the axes, no secure key can be generated, even with dynamic attenuation.

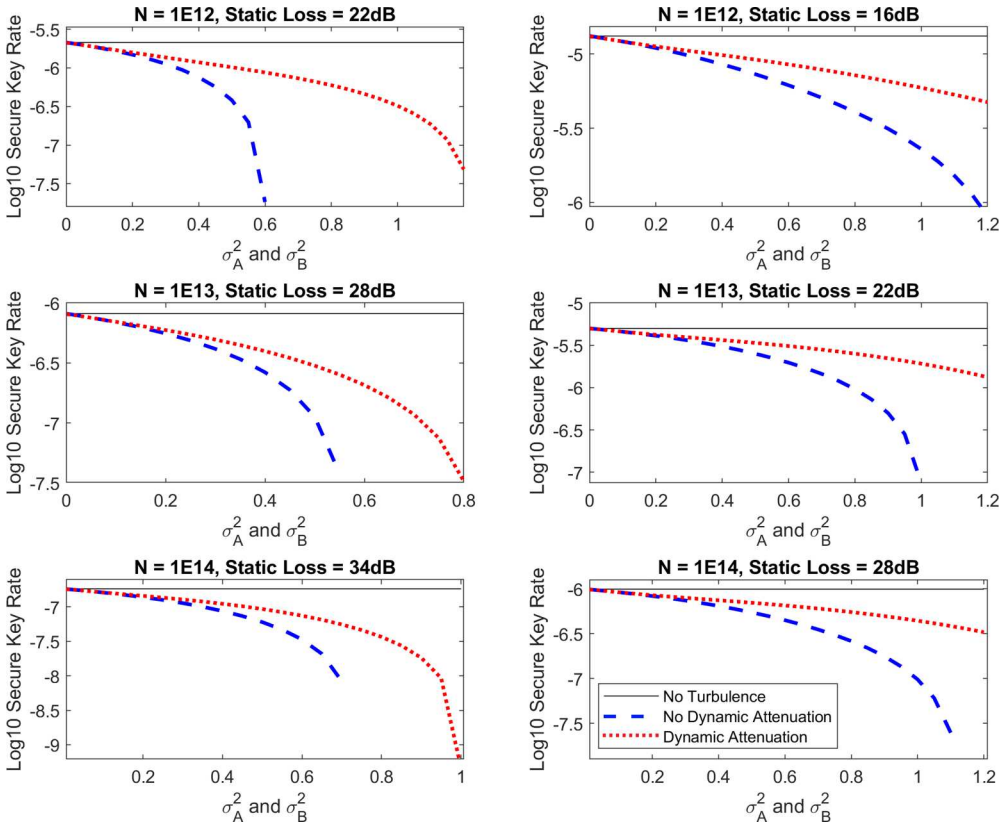

FIG. 6. Key rate using dynamic attenuation (red dotted curves) compared with key rate without dynamic attenuation (blue dashed curves) vs severity of turbulence for various pulse sizes and average losses. Notice the improvement in key rate is better for higher turbulence.

largest benefit can be seen in shorter keys, though there is still an advantage in large ones. Furthermore, if we vary loss and keep $\sigma_A^2 = \sigma_B^2 = 1.0$, we can see an improvement in loss tolerance as shown in Fig. 7.

In the above simulations, we have assumed the minimum loss of the VOA can be set to 0 dB. However, if one considers implementing the high-speed VOA using a commercial $LiNbO_3$amplitude modulator, the minimum insertion loss could be about 2–3 dB. There will be a penalty on secret key rate associated with the minimum insertion loss. Nevertheless, the advantage of the dynamic attenuation scheme at high turbulence remains, as shown in Fig. 8.

Figure 8 shows that dynamic attenuation with nonzero insertion loss is only beneficial beyond a certain level of turbulence. Thus, one should only use dynamic attenuation when the turbulence is high. At low data rates, this could be problematic, but for 1-GHz pulse rates [52], it takes about 15–20 min to send $N = 10^{12}$. In this time frame, it is unlikely that turbulence will change drastically, as shown in Refs. [53–55], so an entire experiment could be completed when turbulence is high and dynamic attenuation is most useful.

TABLE II. Decoy parameters for each of our simulations.

N	dB	s	μ	ν	P_s	P_μ	P_ν
10^{12}	28	0.353	0.229	0.051	0.527	0.055	0.285
10^{13}	34	0.450	0.200	0.037	0.573	0.066	0.219
10^{14}	40	0.499	0.198	0.026	0.466	0.123	0.295

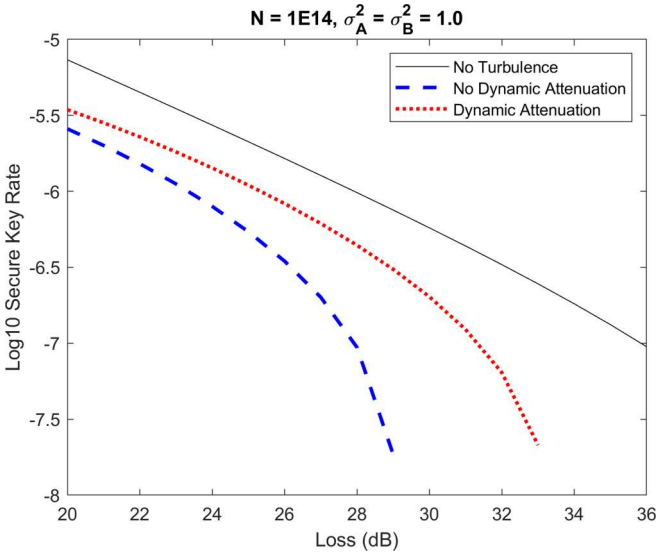

FIG. 7. Dynamic attenuation compared to conventional key rate in a turbulent channel and a static channel for various average losses. The lookup table and decoy parameters for 20-dB loss in each arm were used so a positive key could be achieved for a larger range of losses.

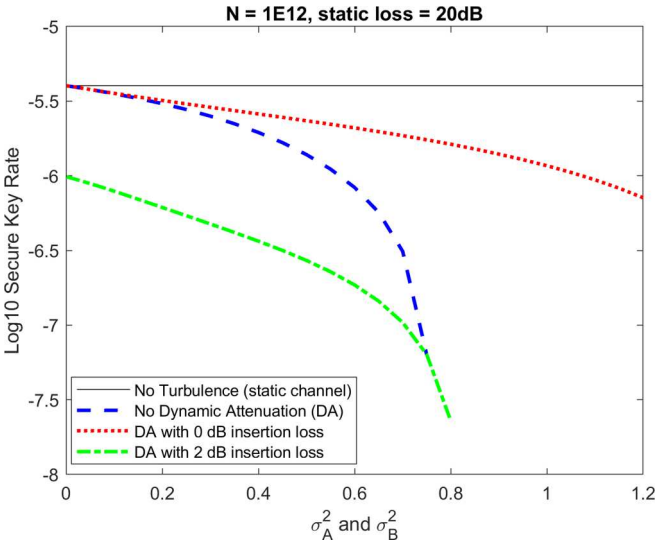

FIG. 8. The impact of the minimum loss of VOA. Secret key rates with dynamic attenuation and minimum loss of 0 dB (red dotted curve) and 2 dB (green dash-dotted curve), and secret key rates without dynamic attenuation (blue dashed curve).

V. CONCLUSION

We introduced the seemingly paradoxical idea that one could enhance the secure key rate of an MDI QKD setup in turbulence by adding loss in one of the channels. We improved the HOM visibility by dynamically adding loss to balance the constantly fluctuating channel transmittances. This dynamic attenuation modified the original joint PDTC to one which was more favorable to MDI QKD.

We remark that classical beacon laser beams are commonly used in free-space QKD for synchronization, polarization alignment, beam tracking, wave-front correction, etc. The same beacon laser beams could also be used as the probe beams to implement our protocol. In this regard, it could be beneficial to first perform the other corrections mentioned above to maximize the transmittance of each individual channel and then apply the dynamic attenuation scheme.[1] Furthermore, dynamic attenuation could be piggybacked off such systems, eliminating the need for additional probe beams.

It should be pointed out that in order to use fiber-based VOAs, one needs VOAs with extremely low loss, because much of the plot area in Fig. 4 shows an optimal attenuation of 0 dB whenever the channels' transmittances are close. Adding too much loss under these conditions could spoil advantages gained through dynamically attenuating less balanced channels. Nevertheless, as shown in Fig. 8, a strong advantage still remains for higher turbulence.

Our results show that secure keys can be obtained for much higher turbulence when one applies dynamic attenuation, especially when using short raw key lengths. We have shown that automated channel transmittance balancing is very helpful in extending MDI QKD's use in a highly turbulent environment.

[1]We thank the anonymous reviewer for the comment.

It would be interesting to derive the kernel K used in our calculations [Eq. (5)] rigorously and apply our method in conjunction with a postselection process [31].

ACKNOWLEDGMENTS

This material is based upon work supported by the U.S. Department of Energy, Office of Science, Office of Advanced Scientific Computing Research, through the Quantum Internet to Accelerate Scientific Discovery Program under Field Work Proposal No. 3ERKJ381.

APPENDIX: NOISE MODEL AND FINITE KEY CALCULATION

Here we describe the model needed to predict the sifted key and error quantities, and then we proceed to compute the finite secure key length using a method described in the Appendix of Ref. [24]. We consider intensities of Alice's and Bob's beams in the set $\{s_{A,B}, \mu_{A,B}, \nu_{A,B}, \omega\}$, where s is the signal, μ and ν are decoy states, and $\omega = 0$ is the vacuum state, assuming perfect intensity modulators. η_D is the detector efficiency for all detectors and $\eta_{A,B}$ are the channel transmittances excluding the detector.

1. Noise model

a. Z basis

The probability of coincidence when Alice and Bob send opposite polarizations is

$$n_{z1} = \tfrac{1}{2}(1-2e_{d,Z})(1-e^{-\eta_A\eta_D s_A})(1-e^{-\eta_B\eta_D s_B}), \quad \text{(A1)}$$

where dark counts are neglected, as well as cases of Alice and Bob both being misaligned. $P_{s_{A,B}}$ and N are suppressed in this step, because they are canceled in the secure key calculation.

Whenever Alice and Bob send the same polarization, the coincident probability is

$$n_{z2} = \tfrac{1}{2}\left(1-e^{-(1-e_{d,Z})\eta_A\eta_D s_A}e^{-(1-e_{d,Z})\eta_B\eta_D s_B}\right) \times (e_{d,Z}\eta_A\eta_D s_A + e_{d,Z}\eta_B\eta_D s_B + 2Y_0). \quad \text{(A2)}$$

We have $n_Z = n_{z1} + n_{z2}$ and $m_X = n_{z2}$.

b. X basis

We refer to each intensity as k_i, where $i = 2$ and 3 are the decoy states, and $i = 4$ is the vacuum. The only coincidences that survive sifting have the same intensity state.

First, consider when Alice and Bob send opposite polarizations. Whenever a single photon is incident at the beam splitter, the only coincidences that are possible are due to dark counts. We have

$$P_{\text{coin}} = \eta_A\eta_D k_{i,A}e^{-\eta_A\eta_D k_{i,A}}Y_0 + \eta_B\eta_D k_{j,B}e^{-\eta_B\eta_D k_{j,B}}Y_0. \quad \text{(A3)}$$

When Alice and Bob each send one photon, we have

$$P_{\text{coin}} = \eta_A\eta_B\eta_D^2 k_{i,A}k_{j,B}e^{-\eta_A\eta_D k_{i,A}-\eta_B\eta_D k_{j,B}}. \quad \text{(A4)}$$

In the case where Alice or Bob sends two photons and the other sends no photons, we have

$$\eta_A\eta_B\eta_D^2 e^{-\eta_A\eta_D k_{i,A}-\eta_B\eta_D k_{j,B}}\frac{k_{i,A}^2 + k_{j,B}^2}{2}. \quad \text{(A5)}$$

Three-photon events are not considered, and so the model loses accuracy at lower losses and high photon numbers.

The number of $|\psi^-\rangle$ events is

$$n_{c1} = \frac{1}{2}\Bigg[\left(\eta_A\eta_D k_{i,A} e^{-\eta_A\eta_D k_{i,A}} Y_0 + \eta_B\eta_D k_{j,B} e^{-\eta_B\eta_D k_{j,B}} Y_0\right) + 0.5\left(\eta_A\eta_B\eta_D^2 k_{i,A}k_{j,B} e^{-\eta_A\eta_D k_{i,A} - \eta_B\eta_D k_{j,B}}\right)(1-2e_{d,X}) + 0.25\left(\eta_A\eta_B\eta_D^2 e^{-\eta_A\eta_D k_{i,A} - \eta_B\eta_D k_{j,B}} \frac{k_{i,A}^2 + k_{j,B}^2}{2}\right)\Bigg], \quad \text{(A6)}$$

and the number of $|\psi^+\rangle$ events is

$$n_{w1} = \frac{1}{2}\Bigg(\left(\eta_A\eta_D k_{i,A} e^{-\eta_A\eta_D k_{i,A}} Y_0 + \eta_B\eta_D k_{j,B} e^{-\eta_B\eta_D k_{j,B}} Y_0\right) + \left(\eta_A\eta_B\eta_D^2 k_{i,A}k_{j,B} e^{-\eta_A\eta_D k_{i,A} - \eta_B\eta_D k_{j,B}}\right)e_{d,X} + 0.25\eta_A\eta_B\eta_D^2 e^{-\eta_A\eta_D k_{i,A} - \eta_B\eta_D k_{j,B}} \frac{k_{i,A}^2 + k_{j,B}^2}{2}\Bigg). \quad \text{(A7)}$$

When Alice and Bob send the same polarization state, the analysis is similar, except with the roles of $|\psi^+\rangle$ and $|\psi^-\rangle$ exchanged. Therefore, $n_{c2} = n_{c1}$ and $n_{w2} = n_{w1}$. Finally, we have

$$\begin{aligned} n_X^{i,j} &= 2(n_{c1} + n_{w1}), \\ m_X^{i,j} &= 2n_{w1}. \end{aligned} \quad \text{(A8)}$$

2. Secure key calculation

The set of probabilities $\{n_Z, n_X, m_Z, m_X\}$ derived above can be used to calculate the secure key rate, by mostly following the steps in the Appendix of Ref. [24]. Having suppressed N and $P_{k_{i,j}}$, the gains are given by

$$\begin{aligned} Q_X^{i,j} &= n_X^{i,j}, \\ T_X^{i,j} &= m_X^{i,j}, \end{aligned} \quad \text{(A9)}$$

where $n_X^{i,j}$ applies to all decoy intensities $i \in \{2, 3, 4\}$. Next, we apply bounds according to $\gamma = 5.3$, the number of standard deviations of an observed value from the expected. This value of γ corresponds to a failure probability of less than 10^{-7}. We have

$$\begin{aligned} \overline{Q_X^{i,j}} &= Q_X^{i,j} + \gamma\sqrt{\frac{Q_X^{i,j}}{NP_{k_i}P_{k_j}}}, \\ \underline{Q_X^{i,j}} &= Q_X^{i,j} - \gamma\sqrt{\frac{Q_X^{i,j}}{NP_{k_i}P_{k_j}}}, \\ \overline{T_X^{i,j}} &= T_X^{i,j} + \gamma\sqrt{\frac{T_X^{i,j}}{NP_{k_i}P_{k_j}}}, \\ \underline{T_X^{i,j}} &= T_X^{i,j} - \gamma\sqrt{\frac{T_X^{i,j}}{NP_{k_i}P_{k_j}}}. \end{aligned}$$

Then, we define

$$\begin{aligned} \underline{Q_{M1}^{\nu\nu}} &= e^{\nu_A+\nu_B}\underline{Q_X^{\nu\nu}} - e^{\nu_A}\overline{Q_X^{\nu\omega}} - e^{\nu_B}\overline{Q_X^{\omega\nu}} + \underline{Q_X^{\omega\omega}}, \\ \underline{Q_{M2}^{\mu\mu}} &= e^{\mu_A+\mu_B}\overline{Q_X^{\mu\mu}} - e^{\mu_A}\underline{Q_X^{\mu\omega}} - e^{\mu_B}\underline{Q_X^{\omega\mu}} + \underline{Q_X^{\omega\omega}}. \end{aligned}$$

We place lower and upper bounds on yield,

$$Y_{X,\min}^{1,1} = \frac{1}{\mu_A - \nu_A}\left(\frac{\mu_A}{\nu_A\nu_B}\underline{Q_{M1}^{\nu\nu}} - \frac{\nu_A}{\mu_A\mu_B}\overline{Q_{M2}^{\mu\mu}}\right), \quad \text{(A10)}$$

and error,

$$e_{X,\max}^{1,1} = \frac{1}{\nu_A\nu_B Y_{X,\min}^{1,1}}(e^{\nu_A+\nu_B}\overline{T_{\nu\nu}} - e^{\nu_A}\underline{T_{\nu\omega}} - e^{\nu_B}\underline{T_{\omega\nu}} + \overline{T_{\omega\omega}}). \quad \text{(A11)}$$

Finally, we define E_z as the error rate in the Z basis. The secure key rate is

$$R = P_{s_A}P_{s_B}\left\{s_A s_B \mathrm{e}^{-(s_A+s_B)} Y_{X,\min}^{1,1}\left[1 - h_2\left(e_{X,\max}^{1,1}\right)\right] - f_{\mathrm{EC}}Q_Z^{1,1}H_2(E_z)\right\}, \quad \text{(A12)}$$

where f_{EC} is the error-correcting efficiency which we set to 1.10, and H_2 is the binary Shannon entropy.

[1] C. H. Bennett and G. Brassard, SIGACT News **20**, 78 (1989).

[2] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, F.-Z. Li, X.-W. Chen, L.-H. Sun, J.-J. Jia, J.-C. Wu, X.-J. Jiang, J.-F. Wang, Y.-M. Huang, Q. Wang, Y.-L. Zhou *et al.*, Nature (London) **549**, 43 (2017).

[3] V. Makarov, New J. Phys. **11**, 065003 (2009).

[4] L. Lydersen, M. Akhlaghi, A. Majedi, J. Skaar, and V. Makarov, New J. Phys. **13**, 113042 (2011).

[5] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, Quantum Inf. Comput. **7**, 73 (2007).

[6] P. Pinheiro, P. Pereira, S. Chaiwongkhot, R. Sajeed, J.-P. Horn, T. Bourgoin, N. Jennewein, V. Lütkenhaus, and Makarov, Opt. Express **26**, 21020 (2018).

[7] N. Jain, B. Stiller, I. Khan, D. Elser, C. Marquardt, and G. Leuchs, Contemp. Phys. **57**, 366 (2016).

[8] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).

[9] J. Barrett, L. Hardy, and A. Kent, Phys. Rev. Lett. **95**, 010503 (2005).

[10] D. Mayers and A. Yao, in *Proceedings 39th Annual Symposium on Foundations of Computer Science* (Cat. No. 98CB36280) (IEEE, New York, 1998), pp. 503–509.

[11] J. S. Bell, Phys. Phys. Fiz. **1**, 195 (1964).

[12] A. Garg and N. D. Mermin, Phys. Rev. D **35**, 3831 (1987).

[13] W. Zhang, T. van Leent, K. Redeker, R. Garthoff, R. Schwonnek, F. Fertig, S. Eppelt, W. Rosenfeld, V. Scarani, C. C.-W. Lim, and H. Weinfurter, Nature (London) **609**, 687 (2022).

[14] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).

[15] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, Phys. Rev. Lett. **111**, 130501 (2013).

[16] Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, and H.-K. Lo, Phys. Rev. Lett. **112**, 190503 (2014).

[17] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang *et al.*, Phys. Rev. Lett. **117**, 190501 (2016).

[18] K. Wei, W. Li, H. Tan, Y. Li, H. Min, W.-J. Zhang, H. Li, L. You, Z. Wang, X. Jiang, T.-Y. Chen, S.-K. Liao, C.-Z. Peng, F. Xu, and J.-W. Pan, Phys. Rev. X **10**, 031030 (2020).

[19] R. Valivarthi, Q. Zhou, C. John, F. Marsili, V. B. Verma, M. D. Shaw, S. W. Nam, D. Oblak, and W. Tittel, Quantum Sci. Technol. **2**, 04LT01 (2017).

[20] C.-K. Hong, Z.-Y. Ou, and L. Mandel, Phys. Rev. Lett. **59**, 2044 (1987).

[21] C. Wang, F. Wang, H. Chen, S. Wang, W. Chen, Z. Yin, D. He, G. Guo, and Z. Han, J. Lightwave Technol. **35**, 4996 (2017).

[22] E. Moschandreou, J. I. Garcia, B. J. Rollick, B. Qi, R. Pooser, and G. Siopsis, J. Lightwave Technol. **36**, 3752 (2018).

[23] F. Xu, M. Curty, B. Qi, and H.-K. Lo, New J. Phys. **15**, 113007 (2013).

[24] W. Wang, F. Xu, and H. K. Lo, Phys. Rev. X **9**, 041012 (2019).

[25] G. R. Osche, *Optical Detection Theory for Laser Applications* (Wiley & Sons, New York, 2002).

[26] C. Erven, B. Heim, E. Meyer-Scott, J. P. Bourgoin, R. Laflamme, G. Weihs, and T. Jennewein, New J. Phys. **14**, 123018 (2012).

[27] I. Capraro, A. Tomaello, A. Dall'Arche, F. Gerlin, R. Ursin, G. Vallone, and P. Villoresi, Phys. Rev. Lett. **109**, 200502 (2012).

[28] G. Vallone, D. G. Marangon, M. Canale, I. Savorgnan, D. Bacco, M. Barbieri, S. Calimani, C. Barbieri, N. Laurenti, and P. Villoresi, Phys. Rev. A **91**, 042320 (2015).

[29] W. Wang, F. Xu, and H.-K. Lo, Phys. Rev. A **97**, 032337 (2018).

[30] E. Moschandreou, B. J. Rollick, B. Qi, and G. Siopsis, Phys. Rev. A **103**, 032614 (2021).

[31] Y. Cao, Phys. Rev. Lett. **125**, 260503 (2020).

[32] W. Wang, F. Xu, and H.-K. Lo, arXiv:1910.10137.

[33] Z.-D. Zhu, D. Chen, S.-H. Zhao, Q.-H. Zhang, and J.-H. Xi, Quantum Inf. Process. **18**, 33 (2019).

[34] E. Biham, B. Huttner, and T. Mor, Phys. Rev. A **54**, 2651 (1996).

[35] H. Inamori, Algorithmica **34**, 340 (2002).

[36] X. Ma, C.-H. F. Fung, and M. Razavi, Phys. Rev. A **86**, 052305 (2012).

[37] F. Kaneda, F. Xu, J. Chapman, and P. G. Kwiat, Optica **4**, 1034 (2017).

[38] Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, J. Wang, K. Cui, H.-L. Yin, N.-L. Liu, L. Li *et al.*, Phys. Rev. Lett. **111**, 130502 (2013).

[39] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, Nat. Photonics **9**, 397 (2015).

[40] T. Ferreira da Silva, D. Vitoreti, G. B. Xavier, G. C. do Amaral, G. P. Temporão, and J. P. von der Weid, Phys. Rev. A **88**, 052303 (2013).

[41] W. Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).

[42] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).

[43] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).

[44] Z.-W. Yu, Y.-H. Zhou, and X.-B. Wang, Phys. Rev. A **91**, 032318 (2015).

[45] Y.-H. Zhou, Z.-W. Yu, and X.-B. Wang, Phys. Rev. A **93**, 042324 (2016).

[46] Z. Ghassemlooy, W. Popoola, and S. Rajbhandari, *Optical Wireless Communications: System and Channel Modelling with Matlab®* (CRC, Boca Raton, FL, 2012).

[47] J. W. Goodman, *Statistical Optics* (Wiley & Sons, New York, 1985).

[48] S. Karp, R. M. Gagliardi, S. E. Moran, and L. B. Stotts, *Optical Channels: Fibers, Clouds, Water, and the Atmosphere* (Springer, Berlin, 2013).

[49] A. Berk, L. S. Bernstein, and D. C. Robertson, *MODTRAN: A Moderate Resolution Model for LOWTRAN*, Technical Report SSI-TR-124 (Spectral Sciences, Inc., Burlington, MA, 1987).

[50] A. Berk, J. van den Bosch, F. Hawes, T. Perkins, P. F. Conforti, G. P. Anderson, R. G. Kennett, and P. K. Acharya, *MODTRAN®6.0.0 (Revision 5) User's Manual* (Spectral Sciences Inc., Burlington, MA, 2016).

[51] H. Smith, D. Dube, M. Gardner, S. Clough, and F. Kneizys, *FASCODE-Fast Atmospheric Signature Code (Spectral Transmittance and Radiance)*, Technical Report No. 2 (VISIDYNE, INC., Burlington, MA, 1978).

[52] L. C. Comandar, M. Lucamarini, B. Fröhlich, J. F. Dynes, A. W. Sharpe, S. W.-B. Tam, Z. L. Yuan, R. V. Penty, and A. J. Shields, Nat. Photonics **10**, 312 (2016).

[53] B. Li, H. Wang, X. Wu, J. Li, and X. Zhang, Optik (Munich, Ger.) **126**, 2726 (2015).

[54] D. Sprung, E. Sucher, A. Ramkilowan, and D. J. Griffith, in *Remote Sensing of Clouds and the Atmosphere XIX; and Optics in Atmospheric Propagation and Adaptive Systems XVII*, Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series, Vol. 9242, edited by A. Comern, K. Stein, E. I. Kassianov, J. D. Gonglewski, and K. Schfer (SPIE, Bellingham, WA, 2014), p. 92421I.

[55] C. Qing, X. Wu, X. Li, Q. Tian, D. Liu, R. Rao, and W. Zhu, Astron. J. **155**, 37 (2018).