Experimental decoy-state asymmetric measurement-device-independent quantum key distribution over a turbulent high-loss channel

Kazi Reaz,[*] Md Mehdi Hassan,[†] Adrien Green,[‡] Noah Crum,[§] and George Siopsis[∥]
Department of Physics and Astronomy, University of Tennessee, Knoxville, Tennessee 37996-1200, USA

(Received 16 November 2023; revised 7 February 2024; accepted 15 March 2024; published 1 April 2024)

Real-world Bennett-Brassard 1984 quantum key distribution (QKD) systems utilize imperfect devices that introduce vulnerabilities to their security, known as side-channel attacks. Measurement-device-independent (MDI) QKD authorizes an untrusted third party to make measurements and removes all side-channel attacks. The typical implementations of MDI QKD employ nearly symmetric channels which are difficult to realize physically in many practical scenarios such as when asymmetric channel losses are present, normally a consequence of the communication environment. Maritime and satellite-based communications are two such instances in which the channels are characterized by continuously changing losses in different channels. In this work we perform asymmetric MDI QKD in a laboratory environment with simulated turbulence using an acousto-optic modulator to interrogate the performance of free-space quantum communication. Under turbulent conditions, scattering and beam wandering cause intensity fluctuations which decrease the detected signal-to-noise ratio. Using the seven-intensity optimization method proposed by Wang *et al.* [Phys. Rev. X **9**, 041012 (2019)], coupled with prefixed-threshold real-time selection (PRTS), we demonstrate enhancement in the secure key rate under turbulent conditions for finite-size decoy-state MDI QKD. Furthermore, we show that PRTS can yield higher secure key rates, particularly in the high-loss regime.

DOI: 10.1103/PhysRevA.109.042603

I. INTRODUCTION

Although quantum key distribution (QKD) has been proven to be unconditionally secure theoretically, practical systems have back doors that Eve can exploit due to device imperfections. In particular, detectors can be attacked through various approaches, such as the blinding-the-detector attack [1], phase-remapping attack [2], time-shift attack [3], as well as through other means (see Ref. [4]). Under these considerations, Lo *et al.* [5] proposed the measurement-device-independent (MDI) QKD protocol, which removes the need for detector security under the condition that Alice and Bob can prepare near-perfect quantum states. Originally, implementations of MDI QKD were performed in nearly symmetric channels [6–12]; however, symmetric channels are difficult to realize in practical scenarios. For example, in a free-space implementation, Alice's and Bob's channels have different losses due to being in geographically different locations. One proposal to balance this asymmetry is to add extra loss in one channel through the addition of extra fiber, which, however, lowers the key rate [12]. Moreover, an MDI QKD implementation in a maritime environment between ships or a satellite-based system will experience continuously changing losses in the different channels that cannot be removed with additional fiber. To overcome these issues, the authors of Refs. [12,13] proposed that asymmetric decoy-state intensities be used to generate a higher key rate instead of adding fiber to one of the channels. Wang *et al.* [14] provided theoretical optimizations for seven different decoy-state intensities that have given the highest expected secure key rates thus far in the literature and have been verified experimentally [15]. In Ref. [16] a long-distance four-intensity free-space implementation with adaptive optics was demonstrated. Among further developments, a robust, multiuser MDI QKD networking scheme was demonstrated in fiber which eliminated reference-frame alignment and polarization compensation need between users [17], and in Ref. [18] it was discovered that asymmetric channel MDI QKD systems have superior secure key rates in systems integrated with classical networks than symmetric MDI QKD.

For our experiment, we conduct simulations to replicate atmospheric effects on traveling pulses, aiming to mimic real-world scenarios. When a signal moves through fiber, attenuation occurs due to various reasons (e.g., absorption or scattering) but the loss remains relatively uniform in time. In contrast, a free-space channel suffers variable attenuation as a result of weather (temperature, clouds, dust, etc.) and altitude. Fortunately, through consideration of the signal's wavelength and the presence of turbulence, there exist well-established models for statistically describing the free-space optical channel.

Erven *et al.* [19] proposed a signal-to-noise-ratio filter in the postprocessing stage to increase the key rate. After data collection, the bits are arranged into time blocks whose duration is adaptive, depending on the detection rate. By optimizing the block duration, an optimum threshold is achieved. In this protocol, the channel loss is assumed to be static

[*] kreaz@vols.utk.edu
[†] mhassa11@vols.utk.edu
[‡] agreen91@vols.utk.edu
[§] ncrum@vols.utk.edu
[∥] siopsis@tennessee.edu

(equal to the mean loss), which may not hold under conditions of strong turbulence and in the high-loss regime.

Vallone *et al.* [20] investigated channel statistics using an auxiliary classical laser beam and found a strong correlation between classical and quantum transmittance data. They created the adaptive real-time selection (ARTS) method, which uses probed channel statistics to postselect bits recorded during high transmittance periods that exceed a certain transmittance threshold. Higher cutoff thresholds improve the signal-to-noise ratio at the expense of reducing the number of available signals, so the optimal threshold is determined in postselection by numerically maximizing the extracted secure key.

A protocol that utilizes a prefixed threshold [prefixed-threshold real-time selection (PRTS)] was introduced theoretically in Ref. [21] and subsequently demonstrated experimentally across different channel losses [22,23] in the context of the finite-key decoy-state Bennett-Brassard 1984 protocol. It was demonstrated in [21] that the optimal threshold is dependent on the transmittance only if the device parameters (e.g., detector efficiency, dark count, and source intensities) remain fixed. Since this threshold can be predetermined, it facilitates real-time data filtering, resulting in savings in storage memory and analysis time when compared to ARTS.

In our experiment, we implement asymmetric MDI QKD following [14]. We use seven asymmetric intensities and the method of decoupled bases in a protocol for asymmetric channels. We analyze the PRTS method in this context using a signal wavelength of 1550 nm and an average channel loss between 30 and 33 dB with moderate turbulence, which we model as a log-normal distribution. We test the theoretical assumptions of the PRTS theory in this context and find significant improvements in the key rate compared to using no data rejection, especially for high loss. It should be noted that there are two spectral windows commonly used in free-space optics, at wavelengths of approximately 850 nm and approximately 1550 nm. We use the latter, for which the atmospheric transmission is higher, especially in urban areas with higher concentration of aerosols, which scatters preferably shorter wavelengths [24,25]. It also coincides with the preferred telecom wavelength, which is convenient as we anticipate future implementations involving both free-space and fiber optics communications. The choice of $\lambda = 1550$ nm comes at the expense of less-efficient single-photon avalanche diodes based on InGaAs/InP which our group used in earlier studies [22,23]. In the present experiments, we use the more expensive, but efficient, superconducting nanowire single-photon detectors.

The structure of this paper is as follows. In Sec. II we discuss the protocol of polarization-encoded MDI QKD including decoy states, and atmospheric turbulence and channel loss implementation. Our experimental setup and all relevant parameters are detailed in Sec. III. Experimental data are presented and compared with simulations in Sec. IV. In Sec. V we present a summary and our conclusions. All essential equations for our calculations can be found in Appendix A. Appendix B details the classical channel we employ.

II. THEORY

Here we describe the theory underpinning MDI QKD and expound upon the instance of asymmetric channels. Specifically, we outline the polarization encoding scheme and describe the implementation of asymmetric MDI QKD using the seven-intensity method introduced in [14]. We also outline the atmospheric model under consideration for severe channel loss with a moderate level of turbulence.

A. Asymmetric MDI QKD

Measurement-device-independent QKD is designed to automatically remove 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 after classical postprocessing. Alice and Bob may choose time-bin encoding [8,26], phase encoding [27], or polarization encoding [6,9,28]. In this work, we use polarization encoding. The Bell-state analyzer in MDI QKD relies on the Hong-Ou-Mandel (HOM) effect [29] 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 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 [9]. With polarization encoding, Alice and Bob encode their random bits on the polarization of their respective weak coherent states, using one of 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 D_{1H}, D_{1V}, D_{2H}, and D_{2V} using a set of four single-photon detectors, and Alice and Bob use the same encoding basis. Since photons are bosons with integer spin, we can write their overall state as $|\Psi\rangle = |\Psi_{\text{spatial}}\rangle \otimes |\Psi_{\text{polarization}}\rangle$. Due to the HOM effect, if the photons come out of opposite sides of the beam splitter, both $|\Psi_{\text{spatial}}\rangle$ and $|\Psi_{\text{polarization}}\rangle$ must be antisymmetric and the polarization state should be $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|HV\rangle - |VH\rangle)$. If the photons come out of the same port, then both must be symmetric, so the polarization state should be $|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|HV\rangle + |VH\rangle)$. The other two possible polarization states $\frac{1}{\sqrt{2}}(|HH\rangle \pm |VV\rangle)$ are not identifiable with our detector setup. When Alice and Bob receive the measurement result from Charlie, they can easily determine the bits they sent. If Charlie announces $|\Psi^+\rangle$ or $|\Psi^-\rangle$ and both Alice and Bob used the rectilinear basis, then one of them has to perform a bit flip to their bit. If both used the diagonal basis and Charlie announces $|\Psi^+\rangle$, then no bit flip is necessary, but if $|\Psi^-\rangle$ is announced, one of them must perform a bit flip. Measurement-device-independent QKD is free from any attack on the detectors, but it is not immune to attacks on sources. So our phase-randomized weak coherent pulses must be protected from the

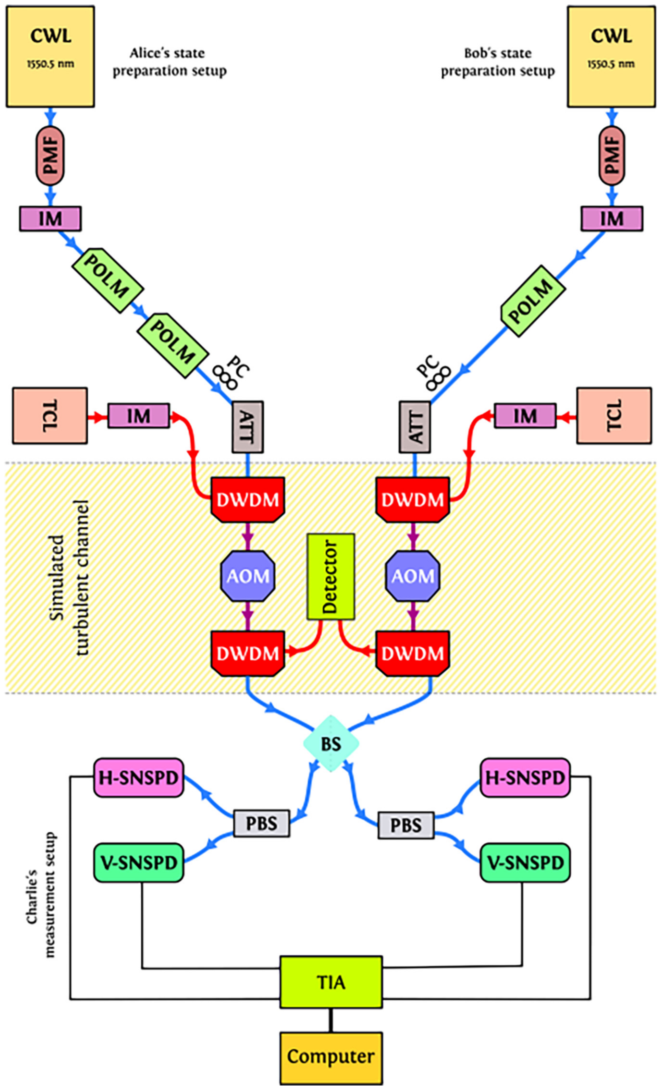


FIG. 1. Schematic of the experimental setup for the asymmetric MDI QKD system. Alice (left) and Bob (right) generate randomly polarized signal pulse trains using a continuous-wave laser (CWL), polarization-maintaining fiber (PMF), intensity modulator (IM), polarization modulator (POLM), and attenuator (ATT). A tunable continuous-wave laser (TCL) with an IM is used to create classical probe pulses. The simulated turbulent channel consists of dense wave division multiplexers (DWDM) and acousto-optic modulators (AOM). Charlie measures the incoming signal using a beam splitter (BS), polarization beam splitters (PBS), superconducting nanowire single-photon detectors (SNSPDs), where 'H' stands for Horizontal polarization detection, 'V' stands for Vertical polarization detection, and a time interval analyzer (TIA) connected to a computer. The color code used to distinguish between fibers is as follows: blue for signal and decoy-state carrying fiber (1550.5-nm laser), red for classical probe pulse carrying fiber (tunable), purple for fiber carrying combined pulses, and black for electronic signal carrying wire.

photon-number-splitting attack. In our laboratory, we use cw laser sources, which have a nonzero probability of multiple photon pulses. To prevent the photon-number-splitting attack, decoy states are implemented [30–32].

In the two-user instance of asymmetric MDI QKD, Alice and Bob utilize quantum channels with asymmetric transmittances η_A and η_B, respectively, where $\eta_A \neq \eta_B$. They must choose optical intensities s_A and s_B, respectively, such that the resulting key rate is maximal [12]. The typical choice is to select intensities obeying $s_A\eta_A = s_B\eta_B$, which ensures a symmetry of photon flux at the relay position, Charlie, providing higher-quality HOM interference [29]. This approach is suboptimal in the asymmetric setting and can even result in a zero key rate for highly asymmetric channels. In particular, HOM interference is dependent on errors only in the X basis, namely, the phase error rate, and not those in the Z basis, the bit error rate. An optimal approach to key generation requires decoupling the decoy-state estimation performed in the X basis from that of the bit generation in the Z basis [14].

In the seven-intensity optimization method of [14], Alice and Bob select a set of four intensities each. These intensities correspond to the signal state intensities $\{s_A, s_B\}$ in the Z basis and the decoy-state intensities in the X basis, $\{\mu_A, \nu_A, \omega\}$ and $\{\mu_B, \nu_B, \omega\}$, for Alice and Bob, respectively. These choices constitute seven separate intensities, each paired with the probability of their preparation. As indicated above, the X basis is reserved for decoy-state analysis, while the Z basis is used to establish the secret key. Therefore, the X-basis intensities are selected to ensure high HOM visibility at the central relay by compensating for the channel asymmetry. This selection provides symmetry of the photon flux at Charlie and roughly satisfies $\frac{\mu_A}{\mu_B} = \frac{\nu_A}{\nu_B} \approx \frac{\eta_B}{\eta_A}$. Due to the decoupling of bases, the signal-state intensity is a free parameter and can be adjusted independently to provide an optimal key rate. In general, this approach does not satisfy $\frac{s_A}{s_B} = \frac{\eta_B}{\eta_B}$. Altogether, Alice and Bob have a set of 12 parameters to optimize, their intensities and the associated probabilities of preparation, namely, $\{s_A, \mu_A, \nu_A, p_{s_A}, p_{\mu_A}, p_{\nu_A}, s_B, \mu_B, \nu_B, p_{s_B}, p_{\mu_B}, p_{\nu_B}\}$.

B. Simulating a turbulent atmosphere

In our experiment, we choose the average channel loss to be at 30 dB as well as 33 dB, which is considered to be severe loss. We choose representative data points in this range because we find no improvement from thresholding at 27 dB of loss or below and we obtain no secure key above 33 dB, even with thresholding. Similarly to our previous work [22,23], we choose the standard and well-accepted log-normal distribution to model the probability distribution of the transmittance coefficient. Mathematically,

$$p_{\eta_0,\sigma}(\eta) = \frac{1}{\sqrt{2\pi}\sigma\eta} \exp\left(-\frac{\left(\ln\frac{\eta}{\eta_0}+\frac{\sigma^2}{2}\right)^2}{2\sigma^2}\right). \quad (1)$$

It depends on two parameters, namely, η_0 (average channel loss) and σ^2 (logarithmic irradiance variance). The latter, commonly known as the Rytov parameter, is correlated with turbulence. It should be noted that transmittance changes significantly on the order of milliseconds [33], typically 8–10 ms. This allows us to consider constant intensity during a data taking session that lasts a much shorter time. If the wavelength remains stable throughout the implementation of the protocol, the plane-wave approximation yields $\sigma^2 = 1.23C_n^2k^{7/6}L^{11/6}$, where k is the wave number, C_n^2 is the refractive index structure parameter (n being the refractive index), and L is the

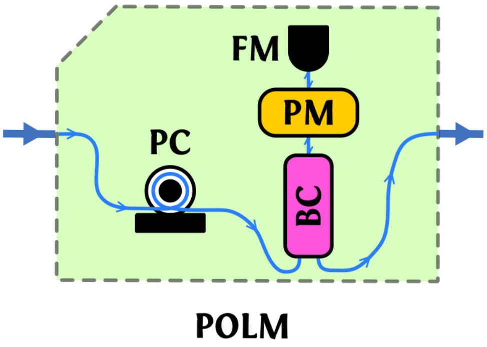


FIG. 2. Details of the polarization modulator (POLM), which consists of a polarization controller (PC), a beam circulator (BC), a phase modulator (PM), and a Faraday mirror (FM).

distance traveled by the wave. While typically C_n^2 is an intricate function influenced by factors such as time of day, local wind conditions, solar elevation angle, and terrain type, most scenarios can be adequately addressed with a simple mathematical relation connecting C_n^2 and altitude.

The intensity distribution (1) due to turbulence is essential for implementing atmospheric effects on quantum channel simulations in the laboratory. We implement it in the simulation of asymmetric channel statistics using an acousto-optic modulator (AOM) integrated with an arbitrary wave-function generator in each channel.

III. EXPERIMENTAL SETUP

Our experimental setup is sketched in Fig. 1(a). To create signals, Alice and Bob use identical continuous-wave lasers as their sources. The semiconductor-based cw lasers are frequency locked at a central wavelength of 1550.5 nm in 2-mW low-power output. Polarization maintaining fiber carries the beam into an intensity modulator. The conversion from continuous wave to pulse train is carried out by a $LiNbO_3$ intensity modulator. The intensity modulators are driven by an arbitrary waveform generator (Tektronix) to control the intensity level of each pulse in order to implement the desired signal and decoy states with different mean photon numbers. In our case, the full width at half maximum (FWHM) pulses are approximately 1ns at a 10-MHz repetition rate. The dc bias voltages are precisely controlled by a null point modulator bias controller device to achieve a high extinction ratio by applying compensation bias voltage.

In the next stage, Alice and Bob encode the desired polarization state into the pulses using polarization modulators. Each polarization modulator consists of a polarization controller, a beam circulator, a phase modulator, and a Faraday mirror (Fig. 2). The phase modulator is driven by an arbitrary wave-function generator. Alice's side contains an extra polarization modulator to align diagonal and antidiagonal polarization [34]. To reach the single-photon level, attenuation is applied to the pulses. In our experiment, we use both digital and manual attenuators. The pulses are attenuated to the single-photon level with the help of variable attenuators. Polarization controllers are utilized by both parties to fine-tune the polarization states to ensure good HOM visibility while calibrating the setup before recording the data.

TABLE I. Optimized parameters.

Channel	Loss (dB)	s	μ	ν	p_s	p_μ	p_ν
			30 dB				
Alice	20	0.617	0.465	0.098	0.590	0.029	0.253
Bob	10	0.169	0.052	0.011	0.607	0.032	0.249
			33 dB				
Alice	20	0.590	0.379	0.081	0.600	0.030	0.240
Bob	13	0.187	0.094	0.020	0.595	0.035	0.244

Next the quantum states are multiplexed with a classical beam with the help of a 200-GHz dense wavelength-division multiplexing (DWDM) device. For the classical signal, we use tunable classical lasers, tuned at 1554 nm. Another set of intensity modulators is used to convert the continuous beam into a pulse train with a pulse rate at 4-kHz repetition at 3-ns FWHM. Classical and quantum signals are mixed in a DWDM device in ITU channels 29 and 33.5, respectively. The classical pulses are used to probe the channel's transmittance statistics. A detailed explanation of estimating the channel's transmittance with classical probe pulses is given in Appendix B. The mixed signals (quantum and classical) are directed into an AOM device independently in each side, which are used to simulate the desired atmospheric channel loss model. The targeted transmittance coefficient distribution, as defined by Eq. (1), is encoded into an `.arb` file. This file is then uploaded to the waveform generator, which in turn controls the AOM devices. In our experiment, Alice's channel suffers a different channel loss as compared to Bob's channel. Another set of DWDM devices is used to filter out (demux) the classical signal from the quantum signal. The classical signal is then detected by a high-gain detector and analyzed with an oscilloscope.

Quantum signals from both sides are fed into a 50:50 beam splitter. Since the setup is properly calibrated, upon interaction, the photons emerge through the output terminal(s) and each basis is resolved by a polarization beam splitter. The outputs of each terminal are detected by superconducting nanowire single-photon detectors (SNSPDs). All the detections of our SNSPDs are recorded by a time interval analyzer (TIA) from IDQ. The TIA is connected to a computer to analyze the count rate of each channel and the coincidence detections among them.

Before conducting the experiment, we calculate the optimized intensities. The signal state intensities s (in the Z basis), decoy-state intensities μ, ν, and ω (in the X basis), and the associated probabilities p_s, p_μ, and p_ν are optimized. The p_ω can be found using the normalization condition $p_s + p_\mu + p_\nu + p_\omega = 1$. We optimize our decoy parameters and probabilities stochastically using a genetic algorithm, which is a preferred technique because it does not require any initial condition. The optimized signal and decoy parameters are given in Table I.

For our experiment, we send 10^{12} pulses and collect data for 27 h at a 10-MHz repetition rate. Prior to the experiment,

TABLE II. Experimental parameters.

Parameter	Value
Number of pulses N	1×10^{12}
Detector efficiency	0.84 ± 0.04
Dead time	~80 ns
Charlie's optical efficiency	0.42 ± 0.02
Time jitter	$\leqslant$50 ps
Polarization error	
Rectilinear basis e_{dZ}	0.004 ± 0.002
Diagonal basis e_{dX}	0.02
Detector dark count probability	
Detector	Probability ($\times 10^{-7}$)
Horizontal ($Y_0^{\leftrightarrow}$)	4.1 ± 0.6
Vertical ($Y_0^{\updownarrow}$)	3.7 ± 0.6
Diagonal ($Y_0^{\nearrow\!\!\!\swarrow}$)	3.2 ± 0.6
Antidiagonal ($Y_0^{\nwarrow\!\!\!\searrow}$)	3.6 ± 0.6

we choose the total number of pulses N, the Z basis misalignment e_d^Z, the X basis misalignment e_d^X, the expected dark counts Y_0, the detector efficiency η_D, an estimated channel transmittance η_0 (as shown in Table II), and the Rytov parameter value to be 1 (moderate turbulence). We then extract the sets $n_{i,j}^X$ and $m_{i,j}^X$, where $i, j = \mu, \nu, \omega$, and calculate the secure key rate using Eq. (3),

$$R = P_{s_A} P_{s_B} \left\{ s_A s_B e^{-(s_A+s_B)} Y_{11}^{X,L} \left[1 - h_2\left(e_{11}^{X,U}\right) \right] - f Q_{ss}^Z h_2\left(E_{ss}^Z\right) \right\}, \tag{2}$$

where $Y_{11}^{X,L}$ is the lower bound of the single-photon yield and $e_{11}^{X,U}$ is the upper bound of the single-photon QBER in the X basis estimated from decoy-state statistics. In addition, Q_{ss}^z and E_{ss}^Z are the gain and QBER, respectively, in the Z basis, which can be determined from experimental data directly. Further, f quantifies the error correction efficiency and h_2 is the binary entropy function, given by $h_2(x) = -x \log_2(x) - (1 - x) \log_2(1 - x)$. More details of the noise model and finite-key calculation for our experiment are available in Appendix A.

IV. ANALYSIS

The main objective of our experiment is to apply PRTS prior to data collection to find a threshold point and compare the resulting secure key rate to the case of no thresholding and to the case of thresholding using ARTS. Adaptive real-time selection is a brute-force optimization, where the secure key rate is calculated repeatedly throughout the whole range of different possible transmittance cutoffs in the log-normal distribution of Eq. (1) and the cutoff giving the highest key rate is chosen. The method therefore gives the highest possible secure key rate but it requires additional processing power and is time consuming. The goal of PRTS is to find the same transmittance cutoff in a predetermined way without the need for real-time data analysis.

First, we compare the PRTS method to performing asymmetric MDI QKD without any transmittance cutoffs. The secure key rate in the first case is calculated by optimizing the data cutoffs for both Alice and Bob as well as their respective decoy-state parameters $\{s_A, \mu_A, \nu_A, p_{s_A}, p_{\mu_A}, p_{\nu_A}, \omega\}$ and $\{s_B, \mu_B, \nu_B, p_{s_B}, p_{\mu_B}, p_{\nu_B}, \omega\}$ and can be done before the experiment begins by taking into account Charlie's detection setup parameters, the average channel loss η_0, and the Rytov parameter σ. Figure 3 shows measured and theoretical secure key rates for the zero-threshold cutoff (static) case and the optimized cutoff case over the examined total mean channel loss. The graph shows that PRTS gives a substantially higher key rate compared to the static case and in particular allows for a key to be generated with approximately 2 dB additional loss. Our experimental secure key rate is very close to the simulation curve in both cases. The reasons for the small deviation are optical misalignment and fluctuation in the average signal and decoy photon number and the difference between measured detector efficiencies. There is an uncertainty of ±0.005 in our setting during the experiment for the desired signal photon number (s_A and s_B) and weak decoy photon number (μ_A, ν_A, ω_A, μ_B, ν_B, and ω_B) given in Table I.

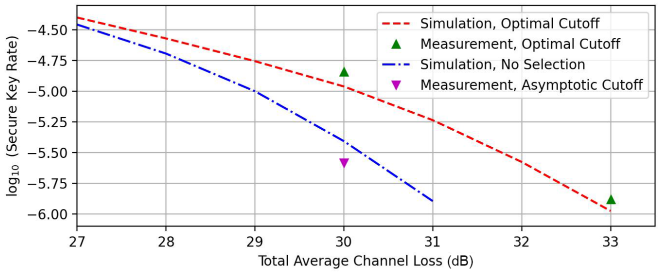
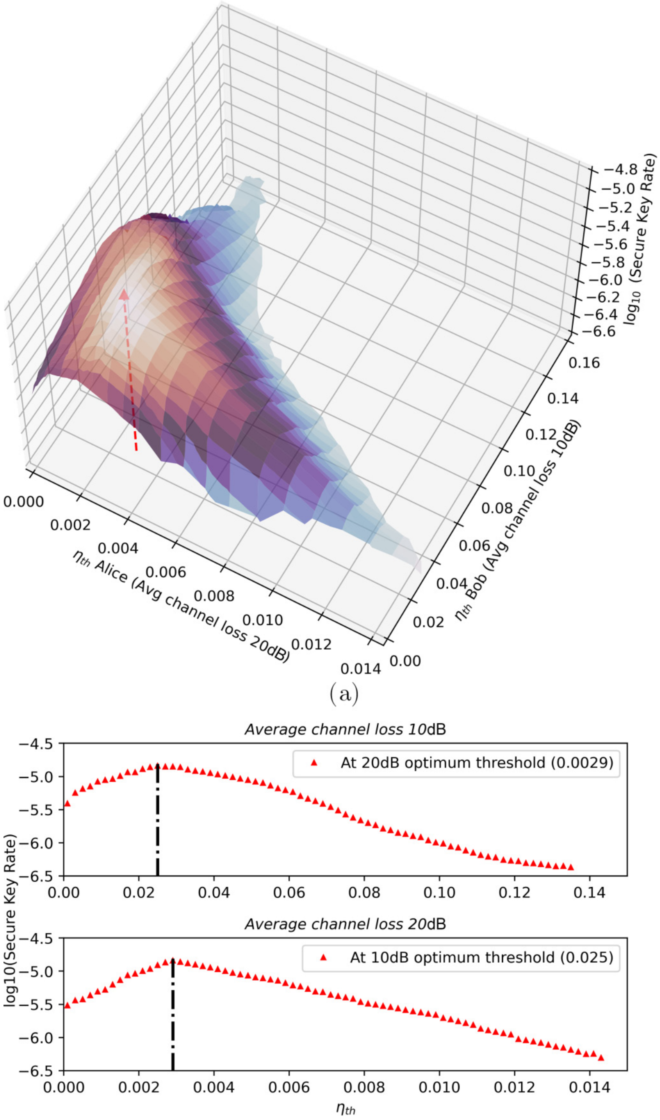


FIG. 3. Using the PRTS method, simulations (dashed lines) and measurements (triangles) were conducted. The secure key rate improves when an optimized cutoff is applied, as compared to the asymptotic cutoff or no selection in both simulation and measurement. The asymptotic cutoff does not generate any practical key rate at 33 dB in either case.

In Fig. 4(a) we show the experimentally measured secure rate for a total mean channel loss of 30 dB, with Alice's channel experiencing an average channel loss of 20 dB and Bob's an average of 10 dB loss using ARTS-type postselection. We note that at this level of asymmetry between the channels, the near-symmetric technique does not generate a secure key [15]. To derive the optimized threshold, we analyze the distilled key rate as a function of threshold transmittance η_{th} for both channels by scanning successive transmittance cutoffs and extract the corresponding secure key rate. The red arrow corresponds to the optimal cutoff that maximizes the key rate, which corresponds to $\eta_{\text{th}} = 0.0029$ for an average channel loss of 20 dB and $\eta_{\text{th}} = 0.025$ for an average channel loss of 10 dB. These results closely match our PRTS results, where we derive $\eta_{\text{th}} = 0.003\,05$ for 20 dB average channel loss and for $\eta_{\text{th}} = 0.026\,33$ for 10 dB average channel loss. The difference in the secure key rate due to the minor change in the threshold values is negligible, showing that the PRTS method allows for a reduction in computation time and resources without a reduction in key rate.

Figure 4(b) shows an example of the cross section of the three-dimensional (3D) plot at optimal cutoff (red triangles). These cross sections are shown to illustrate the optimal cutoff selection point.



(a)

(b)

FIG. 4. Finding an optimal threshold point for asymmetric MDI QKD at a total mean channel loss of 30 dB using an ARTS-type distribution. (a) A 3D plot of all the measurement data points corresponding to ARTS-type postselection where we scanned successive transmittance cutoffs $\eta_{\rm th}$ and extracted the corresponding logarithm of secure key rate R at a total average channel loss of 30 dB. The optimal thresholds are $\eta_{\rm th} = 0.0029$ and 0.025 for Alice and Bob, respectively. (b) Example of the cross section of the 3D plot at the optimal cutoff (red triangle) point.

Figure 5 shows ARTS-type postselection data points for a total of 33 dB average channel loss (Alice at 20 dB and Bob at 13 dB), where again the red arrow points to the optimal cutoff. The PRTS derived optimal cutoffs in this case are $\eta_{\rm th} = 0.003\,01$ for 20 dB average channel loss and $\eta_{\rm th} = 0.025\,84$ for 10 dB average channel loss, which again gives a negligible difference in secure key rate compared to using ARTS thresholds. We note that for both of the loss levels in Figs. 4 and 5, a positive key rate cannot be generated if no transmittance cutoff is used to reject high-loss data.

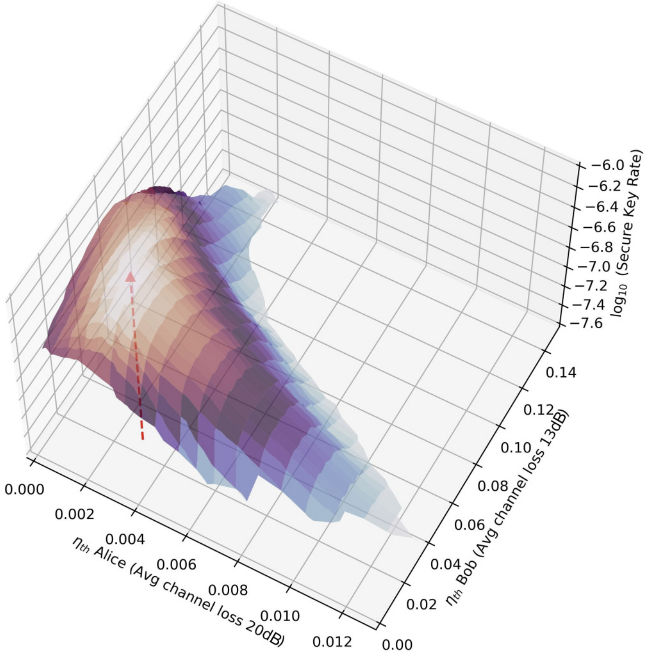


FIG. 5. A 3D plot of ARTS-type measurements, showing the logarithm of the secure key rate R for increasing applied transmittance cutoff $\eta_{\rm th}$ at a total average channel loss of 33 dB, where Alice experiences a 20 dB mean channel loss and Bob experiences a 13 dB mean channel loss.

V. CONCLUSION

We have implemented an experimental demonstration of decoy-state MDI QKD with asymmetric channels in a free-space environment where Alice and Bob are at different distances from Charlie and whose channels experience different channel losses. Our study used a realistic log-normal model to describe moderate atmospheric turbulence.

Our experiment showed that the PRTS method finds the same optimal cutoff that would be found using the ARTS method, demonstrating proof of the PRTS theory in the context of asymmetric, finite-key decoy-state MDI QKD and the secure key rate can be significantly improved in turbulent atmospheric conditions, especially at high loss. This selection method can be seamlessly integrated without major technological upgrades, saving computational resources.

It is worth noting that one could combine both PRTS and ARTS types of selection method depending on the knowledge of the turbulence statistics. The two selection approaches could be employed in conjunction, depending on the knowledge of turbulence statistics. To maximize the extracted secure key rate, a conservative transmittance threshold might be used to perform PRTS-type real-time data rejection, followed by an ARTS-type scan during postselection.

It should be mentioned that our security assumption [35] relies on the random phase of Alice's and Bob's quantum signals, which can be achieved by using phase modulators on both sides [36]. Our setup did not randomize the phase of the quantum signals. However, our detection statistics are practically the same as a phase randomized system because the coherence times of Alice's and Bob's lasers are significantly shorter than the data collection time.

Altogether, overcoming atmospheric turbulence is crucial for establishing a global quantum network and the results presented here further demonstrate the capabilities of QKD systems in harsh environments. It would be interesting to extend our results to other promising protocols, such as twin-field QKD [37,38], and perform experiments to optimize thresholding for free-space implementations of these protocols.

ACKNOWLEDGMENTS

We thank E. Moschandreou and B. Qi for valuable discussions. 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. We also acknowledge support by the National Science Foundation under Award No. DGE-2152168.

APPENDIX A: NOISE MODEL FOR ASYMMETRIC MDI QKD AND FINITE-KEY CALCULATION

In this Appendix we establish a noise model to connect the 13 parameters for secret key calculation with a few QKD system parameters which can be easily calibrated. The QKD system parameters considered here are detector dark count rate or detection efficiency, polarization misalignment in the Z basis, and the HOM visibility in the X basis. Note that HOM visibility depends on both the polarization misalignment in the X basis and the distinguishability of the photons from Alice and Bob. We denote the detector dark count rate by Y_0, detector efficiency by η_d, polarization misalignment in the Z basis (the probability that an H photon goes to a V detector, or vice versa) by e_{dZ}, and HOM visibility in the X basis by V_{HOM}. To quantify the polarization misalignment, we use Charlie's polarization frame as a reference.

1. The Z basis

When Alice and Bob send opposite polarization to Charlie the number of effective detection events

$$n_{z1} = \tfrac{1}{2} N P_{s_A} P_{s_B} (1 - e^{-\eta_A \eta_d s_A})(1 - e^{-\eta_B \eta_d s_B})(1 - 2e_{dZ}).$$

The number of effective detection events when both Alice and Bob send the same polarization

$$\begin{aligned} n_{z2} =& \tfrac{1}{2} N P_{s_A} P_{s_B} (1 - e^{-(1-e_{dZ})\eta_A \eta_d s_A} e^{-(1-e_{dZ})\eta_B \eta_d s_B}) \\ & \times (e_{dZ} \eta_A \eta_d s_A + Y_0 + e_{dZ} \eta_B \eta_d s_B + Y_0). \end{aligned}$$

We denote the total detection count by n_{ss}^Z and the error count by m_{ss}^Z in the Z basis. Here $n_{ss}^Z = n_{z1} + n_{z2}$ and $m_{ss}^Z = n_{z2}$.

2. The X basis

We denote by $n_{i,j}^X$ the total number of detections given that Alice prepared i photon states in the X basis and Bob prepared j photon states in the X basis ($i, j = \mu, \nu, \omega$). In the X basis, the correct detection for $\{A, D\}$ and $\{D, A\}$ is $|\Psi^-\rangle$, while the correct detection for $\{A, A\}$ and $\{D, D\}$ is $|\Psi^+\rangle$. When Alice and Bob prepare $\{A, D\}$ or $\{D, A\}$ we consider three cases based on the photon number arrived at by the detectors: For the $\{1, 0\}$ and $\{0, 1\}$ case the corresponding probability of $|\Psi^-\rangle$ events is

$$Y_0(\eta_d \eta_A \mu_A + \eta_d \eta_B \omega_B) e^{-\eta_A \eta_d \mu_A - \eta_B \eta_d \omega_B}$$

and the corresponding probability of $|\Psi^+\rangle$ events is

$$Y_0(\eta_d \eta_A \mu_A + \eta_d \eta_B \omega_B) e^{-\eta_A \eta_d \mu_A - \eta_B \eta_d \omega_B};$$

for the $\{1, 1\}$ case the corresponding probability of $|\Psi^-\rangle$ events is

$$\tfrac{1}{2}(1 - 2e_{dX}) \eta_A \eta_d \mu_A \eta_B \eta_d \omega_B e^{-\eta_A \eta_d \mu_A - \eta_B \eta_d \omega_B}$$

and the corresponding probability of $|\Psi^+\rangle$ events is

$$\tfrac{1}{4}(1 - 2e_{dX}) \eta_d \eta_A \mu_A \eta_d \eta_B \mu_B e^{-\mu_A \eta_d \mu_A - \eta_B \eta_d (\mu_A + \omega_B)};$$

and for the $\{2, 0\}$ and $\{0, 2\}$ case the corresponding probability of $|\Psi^-\rangle$ events is

$$\tfrac{1}{4}[(\eta_d \eta_A \mu_A)^2 + (\eta_d \eta_B \omega_B)^2] e^{-\mu_A \eta_d \mu_A - \eta_B \eta_d \omega_B}$$

and the corresponding probability of $|\Psi^+\rangle$ events is

$$\tfrac{1}{4} e_{dX} [(\eta_d \eta_A \mu_A)^2 + (\eta_d \eta_B \omega_B)^2] e^{-\mu_A \eta_d \mu_A - \eta_B \eta_d \omega_B}.$$

Combining these three cases, we obtain the total number of $|\Psi^-\rangle$ events

$$\begin{aligned} n_{c_1} =& \tfrac{1}{2} N P_{\mu_A} P_{\omega_B} \{ Y_0(\eta_d \eta_A \mu_A + \eta_d \eta_B \omega_B) e^{-\eta_A \eta_d \mu_A - \eta_B \eta_d \omega_B} + \tfrac{1}{2}(1 - 2e_{dX}) \eta_A \eta_d \mu_A \eta_B \eta_d \omega_B e^{-\eta_A \eta_d \mu_A - \eta_B \eta_d \omega_B} \\ & + \tfrac{1}{4}[(\eta_d \eta_A \mu_A)^2 + (\eta_d \eta_B \omega_B)^2] e^{-\mu_A \eta_d \mu_A - \eta_B \eta_d \omega_B} \} \end{aligned}$$

and the total number of $|\Psi^+\rangle$ events

$$\begin{aligned} n_{w_1} =& \tfrac{1}{2} N P_{\mu_A} P_{\omega_B} \{ Y_0(\eta_d \eta_A \mu_A + \eta_d \eta_B \omega_B) e^{-\eta_A \eta_d \mu_A - \eta_B \eta_d \omega_B} + \tfrac{1}{4}(1 - 2e_{dX}) \eta_d \eta_A \mu_A \eta_d \eta_B \mu_B e^{-\mu_A \eta_d \mu_A - \eta_B \eta_d (\mu_A + \omega_B)} \\ & + \tfrac{1}{4} e_{dX} [(\eta_d \eta_A \mu_A)^2 + (\eta_d \eta_B \omega_B)^2] e^{-\mu_A \eta_d \mu_A - \eta_B \eta_d \omega_B} \}. \end{aligned}$$

When Alice and Bob prepare $\{D, D\}$ or $\{A, A\}$, the analysis will be similar to $\{A, D\}$ or $\{D, A\}$, except the roles of $|\Psi^+\rangle$ and $|\Psi^-\rangle$ are interchanged. Here $n_{c_2} = n_{c_1}$ and $n_{w_2} = n_{w_1}$. Therefore, $n^X_{i,j} = 2(n_{c_1} + n_{w_1})$ and $m^X_{i,j} = 2n_{w_1}$.

Combining the above, we obtain the total number of detection counts

$$n^X_{\mu\omega} = NP_{\mu_A}P_{\omega_B}[2Y_0(\eta_d\eta_A\mu_A + \eta_d\eta_B\omega_B)e^{-\eta_A\eta_d\mu_A-\eta_B\eta_d\omega_B} + \tfrac{1}{4}(\eta_d\eta_A\mu_A + \eta_d\eta_B\omega_B)^2e^{-\eta_A\eta_d\mu_A-\eta_B\eta_d\omega_B}].$$

Combining the above, we obtain the total number of error counts

$$m^X_{\mu\omega} = NP_{\mu_A}P_{\omega_B}\{Y_0(\eta_d\eta_A\mu_A + \eta_d\eta_B\omega_B)e^{-\eta_A\eta_d\mu_A-\eta_B\eta_d\omega_B} + \tfrac{1}{8}[(\eta_d\eta_A\mu_A)^2 + (\eta_d\eta_B\omega_B)^2 + 8e_{dX}\eta_d\eta_A\mu_A\eta_d\eta_B\omega_B]e^{-\eta_A\eta_d\mu_A-\eta_B\eta_d\omega_B}\}.$$

All the other terms can be determined by simply replacing all possible average photon numbers with the corresponding combinations of μ, ν, and ω.

3. Finite-key calculation

Next we account for the finite-size effect using standard error analysis [12]. We denote the observed total counts and error counts by $n^X_{i,j}$ and $m^X_{i,j}$, respectively, where $i, j = \mu, \nu, \omega$. The corresponding gains are

$$Q^X_{i,j} = \frac{n^X_{i,j}}{NP_{i_A}P_{j_B}}$$

and the errors are given by

$$E^X_{i,j} = \frac{T^X_{i,j}}{Q^X_{i,j}}, \quad T^X_{i,j} = \frac{m^X_{i,j}}{NP_{i_A}P_{j_B}}.$$

The upper and lower bounds of gains and errors are

$$\overline{Q^X_{i,j}} = Q^X_{i,j} + \gamma\sqrt{\frac{Q^X_{i,j}}{NP_{i_A}P_{j_B}}},$$

$$\underline{Q^X_{i,j}} = Q^X_{i,j} - \gamma\sqrt{\frac{Q^X_{i,j}}{NP_{i_A}P_{j_B}}},$$

$$\overline{T^X_{i,j}} = T^X_{i,j} + \gamma\sqrt{\frac{T^X_{i,j}}{NP_{i_A}P_{j_B}}},$$

$$\underline{T^X_{i,j}} = T^X_{i,j} - \gamma\sqrt{\frac{T^X_{i,j}}{NP_{i_A}P_{j_B}}},$$

where γ is related to the failure probability ϵ via $\epsilon = \mathrm{erfc}(\frac{\gamma}{\sqrt{2}})$. We choose $\gamma = 5.3$ so that $\epsilon \lesssim 10^{-7}$. The lower bound of yield $Y^{X,L}_{11}$ is estimated as

$$Y^{X,L}_{11} = \frac{1}{\mu-\nu}\left(\frac{\mu+\omega}{(\nu-\omega)^2}\underline{Q^{M1}_{\nu\nu}} + \frac{\nu+\omega}{(\mu-\omega)^2}\overline{Q^{M2}_{\mu\mu}}\right),$$

where

$$\underline{Q^{M1}_{\nu\nu}} = e^{2\nu}\underline{Q^X_{\nu\nu}} + e^{2\omega}\underline{Q^X_{\omega\omega}} + e^{\nu+\omega}\overline{Q^X_{\nu\omega}} + e^{\omega+\nu}\overline{Q^X_{\omega\nu}},$$

$$\overline{Q^{M2}_{\mu\mu}} = e^{2\mu}\overline{Q^X_{\mu\mu}} + e^{2\omega}\underline{Q^X_{\omega\omega}} - e^{\mu+\omega}\underline{Q^X_{\mu\omega}} - e^{\omega+\mu}\underline{Q^X_{\omega\mu}}.$$

The upper bound of error $e^{X,U}_{11}$ is estimated as

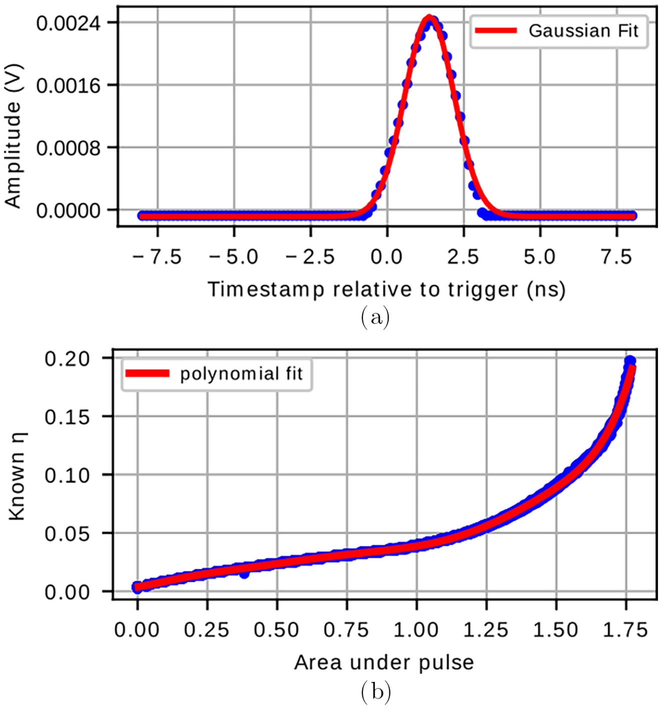
$$e^{X,U}_{11} = \frac{e^{2\nu}\overline{T^X_{\nu\nu}} + e^{2\omega}\overline{T^X_{\omega\omega}} - e^{\nu+\omega}\underline{T^X_{\nu\omega}} - e^{\omega+\nu}\underline{T^X_{\omega\nu}}}{(\mu-\nu)Y^{X,L}_{11}}.$$

The final secure key rate is

$$R = P_{s_A}P_{s_B}\{Y^{X,L}_{11}s_As_Be^{-(s_A+s_B)}[1 - h_2(e^{X,U}_{11})] - fQ^Z_{ss}h_2(E^Z_{ss})\}. \tag{A1}$$

APPENDIX B: CLASSICAL CHANNEL

To estimate the channel's transmittance with classical probe pulses we follow the same procedure as in [22]. In our experimental setup, the classical probe pulses are set at a repetition rate of 4 kHz and a FWHM of approximately 3 ns. The laser power of the classical channel is 7 dBm. The classical pulses are sent along with quantum pulses to the AOM using ITU channel 29. After reaching the AOM, the classical pulses are separated from the quantum pulses using a DWDM. The classical pulses are then sent to the high-gain classical photodetector, which is connected to the DPO 7205 Tektronix Oscilloscope. The oscilloscope has a fast-frame feature to store high-resolution pulse data in a short (16-ns) interval around the trigger, sampled at 5 gigasamples per second [Fig. 6(a)]. A Gaussian fit is performed on



(a)

(b)

FIG. 6. Using classical probe pulses to estimate the quantum channel's transmittance. (a) Example of the Gaussian fit of a classical probe pulse obtained using the oscilloscope's fast-frame feature. (b) Correlation between the programmed transmittance and the area under the pulse using a polynomial fit.

the measured classical pulses in order to calculate the area under the pulse to quantify the intensity. Finally, the transmittance is extracted from the measured pulse area using a polynomial fit. Figure 6(b) shows that a similar resolution can be achieved by summing all the samples of each frame, with a significantly faster computation time than the Gaussian fit procedure.

It should be noted that in our experimental setup, quantum and classical signals travel together a distance of approximately 5m. This is too short a distance to observe any Raman scattering for which a fiber over 1 km long is needed. In a real-life implementation of our experiment, the classical channel will be a separate channel used to estimate channel transmittance.

[1] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photonics **4**, 686 (2010).

[2] C.-H. F. Fung, B. Qi, K. Tamaki, and H.-K. Lo, Phys. Rev. A **75**, 032314 (2007).

[3] C.-H. F. Fung, K. Tamaki, B. Qi, H.-K. Lo, and X. Ma, Quant. Inf. Comput. **9**, 131 (2009).

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

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

[6] 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).

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

[8] 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, X. Ma, J. S. Pelc, M. M. Fejer, C.-Z. Peng, Q. Zhang, and J.-W. Pan, Phys. Rev. Lett. **111**, 130502 (2013).

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

[10] Y.-L. Tang, H.-L. Yin, S.-J. Chen, Y. Liu, W.-J. Zhang, X. Jiang, L. Zhang, J. Wang, L.-X. You, J.-Y. Guan, D.-X. Yang, Z. Wang, H. Liang, Z. Zhang, N. Zhou, X. Ma, T.-Y. Chen, Q. Zhang, and J.-W. Pan, Phys. Rev. Lett. **113**, 190501 (2014).

[11] 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, H. Chen, M. J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X.-B. Wang, and J.-W. Pan, Phys. Rev. Lett. **117**, 190501 (2016).

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

[13] X.-B. Wang, Phys. Rev. A **87**, 012320 (2013).

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

[15] H. Liu, W. Wang, K. Wei, X.-T. Fang, L. Li, N.-L. Liu, H. Liang, S.-J. Zhang, W. Zhang, H. Li, L. You, Z. Wang, H.-K. Lo, T.-Y. Chen, F. Xu, and J.-W. Pan, Phys. Rev. Lett. **122**, 160501 (2019).

[16] Y. Cao, Y.-H. Li, K.-X. Yang, Y.-F. Jiang, S.-L. Li, X.-L. Hu, M. Abulizi, C.-L. Li, W. Zhang, Q.-C. Sun *et al.*, Phys. Rev. Lett. **125**, 260503 (2020).

[17] G.-J. Fan-Yuan, F.-Y. Lu, S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, Z. Zhou, Z.-H. Wang, J. Teng, G.-C. Guo *et al.*, Optica **9**, 812 (2022).

[18] W.-X. Xie, G.-J. Fan-Yuan, Z.-H. Wang, F.-Y. Lu, J.-X. Li, S. Wang, Z.-Q. Yin, W. Chen, D.-Y. He, G.-C. Guo *et al.*, Phys. Rev. Appl. **20**, 054042 (2023).

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

[20] 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).

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

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

[23] M. M. Hassan, K. Reaz, A. Green, N. Crum, and G. Siopsis, in *2023 IEEE International Conference on Quantum Computing and Engineering (QCE), Bellevue, 2023*, edited by H. Muller, Y. Alexev, A. Delgado, and G. Byrd (IEEE, Piscataway, 2023), Vol. 1, pp. 1182–1186.

[24] M. J. García-Martínez, N. Denisenko, D. Soto, D. Arroyo, A. B. Orue, and V. Fernandez, Appl. Opt. **52**, 3311 (2013).

[25] M. Abasifard, C. Cholsuk, R. G. Pousa, A. Kumar, A. Zand, T. Riel, D. K. L. Oi, and T. Vogl, arXiv:2303.02106.

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

[27] 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).

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

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

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

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

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

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

[34] Z. Tang, K. Wei, O. Bedroya, L. Qian, and H.-K. Lo, Phys. Rev. A **93**, 042308 (2016).

[35] H.-K. Lo and J. Preskill, Quant. Inf. Comput. **7**, 431 (2007).

[36] Y. Zhao, B. Qi, and H.-K. Lo, Appl. Phys. Lett. **90**, 044106 (2007).

[37] S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, R.-Q. Wang, P. Ye, Y. Zhou, G.-J. Fan-Yuan, F.-X. Wang, W. Chen *et al.*, Nat. Photonics **16**, 154 (2022).

[38] Y. Yu, R. Xu, L. Wang, Q. Mao, and S. Zhao, Entropy **24**, 344 (2022).