Experimental decoy-state Bennett-Brassard 1984 quantum key distribution through a turbulent channel

Eleftherios Moschandreou,[1,*] Brian J. Rollick,[1,†] Bing Qi,[2,‡] and George Siopsis[1,§]
[1]*Department of Physics and Astronomy, University of Tennessee, Knoxville, Tennessee 37996-1200, USA*
[2]*Quantum Information Science Group, Computational Sciences and Engineering Division, Oak Ridge National Laboratory, Oak Ridge, Tennessee 37831-6418, USA*

(Received 23 January 2021; accepted 11 March 2021; published 26 March 2021)

In free-space quantum key distribution (QKD) in turbulent conditions, scattering and beam wandering cause intensity fluctuations which decrease the detected signal-to-noise ratio. This effect can be mitigated by rejecting received bits when the channel's transmittance is below a threshold. Thus, the overall error rate is reduced and the secure key rate increases despite the deletion of bits. In this work, we implement recently proposed selection methods focusing on the prefixed-threshold real-time selection (P-RTS) where a cutoff can be chosen prior to data collection and independently of the transmittance distribution. We perform finite-size decoy-state Bennett-Brassard 1984 QKD in a laboratory setting where we simulate the atmospheric turbulence using an acousto-optical modulator. We show that P-RTS can yield considerably higher secure key rates for a wide range of the atmospheric channel parameters. In addition, we evaluate the performance of the P-RTS method for a realistically finite sample size. We demonstrate that a near-optimal selection threshold can be predetermined even with imperfect knowledge of the channel transmittance distribution parameters.

DOI: 10.1103/PhysRevA.103.032614

I. INTRODUCTION

As quantum communication grows from proof-of-principle laboratory demonstrations towards large-scale commercial deployment, a lot of attention is focused on the optical medium on which such networks can be realized.

Today, quantum communication through fiber-optical networks is possible at metropolitan scales [1,2], but limited in distance due to transmission losses, typically ∼0.2 dB/km at 1550 nm wavelength [3]. While classical optical signals can be enhanced by intermediate amplifiers and reach far larger distances, such techniques cannot be employed to amplify quantum signals due to the no-cloning theorem [4]. Quantum repeaters [5] are a possible solution, but much progress needs to be made before they become available for practical quantum communication. Free-space channels offer an attractive alternative at intermediate distances for mobile communication, remote communicating parties, or as part of a ground-to-satellite network. So far, experimental demonstrations in free space include ground-to-airplane [6,7], hot-air balloon [8], and drones [9], as well as multiple studies on the feasibility of ground-to-satellite quantum communication [8,10–13] and the launch of a quantum key distribution (QKD) dedicated satellite [14–16].

Signals traveling in free space experience losses due to turbulence, atmospheric absorption, and scattering, and consequentially experience consistent degradation of the signal intensity. Caused by fluctuations in the air temperature and pressure, turbulent eddies of various sizes produce random variations in the atmospheric refractive index, which cause beam wandering and deformation of the beam front [17,18].

The description of light propagation in a turbulent medium is a very difficult problem, but the channel can be described statistically. It is commonly accepted that the transmission coefficient can be approximated by a log-normal probability distribution at moderate turbulence [19–21], and by a gamma-gamma distribution at higher turbulence [22,23]. However, most work to date treats the effect of turbulence on the transmittance as an average loss, without considering the details of the distribution of the transmission coefficient.

Taking the channel statistics into account, various selection methods that reject or discard recorded bits when the channel transmittance is low have been recently proposed. Evren *et al.* [24] developed a signal-to-noise-ratio (SNR) filter where the detected quantum signals are grouped into bins during post-processing. Any bins with a detection rate below a certain threshold are discarded. To maximize the secure key rate, a searching algorithm was developed to find the optimal bin size and cutoff threshold.

Vallone *et al.* [25] employed an auxiliary classical laser beam to probe the channel statistics and observed good correlation between the classical and quantum transmittance data. They developed the adaptive real-time selection (ARTS) method, where the probed channel statistics are used to postselect bits recorded during high transmittance periods, above a certain transmittance threshold. Higher cutoff thresholds improve the SNR at the cost of reducing the number of available signals so the optimal threshold is determined

*emoschan@vols.utk.edu
†brollick@vols.utk.edu
‡qib1@ornl.gov
§siopsis@tennessee.edu

by numerically maximizing the extracted secure key in postselection.

Wang *et al.* [26] proposed the prefixed-threshold real-time selection (P-RTS) method and showed that the optimal selection threshold is insensitive to the channel statistics. Rather, it depends primarily on the receiver's detection setup characteristics (i.e., the detection efficiency and background noise) and less strongly on the intensity of the quantum signals. Thus, the threshold can be predetermined without knowledge of the channel statistics, and the rejection of the recorded bits can be accomplished in real time without the need to store unnecessary bits or perform additional postprocessing. The P-RTS method was extended to the measurement-device-independent QKD (MDI QKD) [27] protocol in recent studies [28,29]. In particular, Ref. [29] highlights the importance of applying a selection method in MDI QKD as the turbulence impacts the protocol's efficiency, not only through the SNR but also through the asymmetry between the channels that the communicating parties (Alice and Bob) each use to access the middleman (Charles).

In this study, the P-RTS method is employed experimentally on the finite-size decoy-state Bennett-Brassard 1984 (BB84) [30,31] QKD protocol and compared to the optimal key rate found through ARTS. The random transmittance fluctuations caused by the atmospheric turbulence are simulated using an acousto-optical modulator (AOM). We demonstrate that the P-RTS method significantly increases the secure key rate compared to the case of not using postselection, for a wide range of the channel's parameters. Performing the experiments in a laboratory environment allows the study of different atmospheric conditions in a controllable and reproducible manner and this work extends the array of studies that explore aspects of turbulent quantum communication channels with in-laboratory or simulated methods [32–35].

In Sec. II, we review the features of the P-RTS method [26] and discuss how atmospheric effects might alter a free-space communication channel. In Sec. III, we describe our experimental setup and procedure. We outline the key generation analysis and present our results in Sec. IV. Finally, in Sec. V, we offer concluding remarks.

II. THEORY

In this section, we review the main results of the P-RTS method [26] and discuss the atmospheric conditions which might produce our simulated effects.

A. Modeling a turbulent atmosphere

It is accepted that weak to moderate turbulence causes the transmittance coefficient of light propagating in air, η, to fluctuate following a log-normal distribution [36]. The probability density of the transmittance coefficient (PDTC) is given by

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

where η_0 is the average transmittance and σ^2 is the logarithmic irradiance variance, which characterizes the severity of the turbulence. A larger σ^2 indicates a greater transmittance fluctuation. If the length L of the channel is known and the height is constant, σ^2 for a plane wave can be calculated through the relation $\sigma^2 = 1.23C_n^2k^{7/6}L^{11/6}$, where k is the wave number and C_n^2 is the refractive index structure constant, which could be measured using a scintillometer. Because we are treating the height as a constant, we can assume C_n^2 is constant over the channel [37]. Typical values for C_n^2 generally range from 10^{-17} to 10^{-12} $\mathrm{m}^{2/3}$ (going from weak to strong turbulence), with a typical value being $\sim 10^{-15}$ $\mathrm{m}^{2/3}$ [38]. For example, when $C_n^2 = 5\times10^{-15}\,\mathrm{m}^{-2/3}$, i.e., a value which corresponds to moderate turbulence, we arrive at $\sigma = 0.9$ in a 3 km channel given our 1550 nm wavelength. This choice of σ is consistent with prior work (see, e.g., [25]). A similar distribution would be produced if one were to choose a longer channel, albeit with less turbulence. Indeed, in [25], $\sigma = .991$ was measured for a 143 km channel.

It should be pointed out that in the case of strong turbulence ($\sigma^2 \gtrsim 1.2$), the log-normal distribution breaks down [23,36]. Because we argue that P-RTS can predict a cutoff which is largely independent of the PDTC, our findings are also valid in a higher-turbulence scenario.

In addition to turbulence, the beam will be attenuated by the atmosphere. Different software packages such as FASCODE [39] and MODTRAN [40] have been developed to model the atmospheric transmittance as a function of wavelength. In this work, we use MODTRAN to inform our choice of atmospheric loss because it takes into account a number of different transition lines for many airborne compounds and simulates the effects of a plethora of different aerosols, such as oceanic mist and even volcanic debris [41]. In our case, a 3 km channel with 13–19 dB of loss can be produced using a Navy Maritime aerosol model, where visibility ranges from about 1.8 to 2.5 km, a range which corresponds to light fog or hazy conditions. For comparison, 30 dB of loss was obtained for the much longer channel (143 km) between the Tenerife and La Palma islands in [21].

B. Key generation in a turbulent channel

Our experimental setup implements a process in which two users, Alice and Bob, are generating a shared secure key to use for their secret communication. Alice is sending phase-randomized weak coherent (laser) pulses where her bits are encoded as the polarization state. Bob receives and detects the pulses using single-photon avalanche detectors (SPADs). Note that in both the theoretical calculation and the experimental demonstration, while the average channel loss is assumed to be a constant, the channel loss itself fluctuates according to Eq. (1). This channel model has been widely adopted in free-space QKD.

1. Asymptotic case

Following the discussion of [26], to describe the dependence of the secure key generation rate R on the transmittance η of the atmospheric channel, we fix all of Alice's decoy-state parameters as well as all of Bob's detection parameters (i.e., his detectors' efficiencies, background noise, and optical misalignment). Details on the optimization process are given in Appendix A. Then the key rate can be written as a single function of the transmittance, $R(\eta)$.

The maximum key rate $R_{\max}$ that can be extracted using the channel's statistics is given by the convolution of the PDTC, $p_{\eta_0,\sigma}(\eta)$, in Eq. (1) with the rate $R(\eta)$,

$$R_{\max} = \int_0^1 R(\eta) p_{\eta_0,\sigma}(\eta) d\eta. \tag{2}$$

While evaluating this integral is challenging in practical applications, we can set a transmittance threshold $\eta_{\rm TH}$ below which recorded bits are discarded and keep only a fraction $\int_{\eta_{\rm TH}}^1 p_{\eta_0,\sigma}(\eta)d\eta$ of the sent signals. We treat the remaining recordings as having passed through a static channel of average transmittance $\langle\eta\rangle$, computed only from the transmittances above the threshold,

$$\langle\eta\rangle = \frac{\int_{\eta_{\rm TH}}^1 \eta p_{\eta_0,\sigma}(\eta)d\eta}{\int_{\eta_{\rm TH}}^1 p_{\eta_0,\sigma}(\eta)d\eta}. \tag{3}$$

Then the postselected bits produce a key rate [26],

$$R(\eta_{\rm TH}) = R(\langle\eta\rangle) \times \int_{\eta_{\rm TH}}^1 p_{\eta_0,\sigma}(\eta)d\eta. \tag{4}$$

Equation (4) presents an optimization problem: higher cutoffs η_T improve the SNR for the postselected bits and, hence, the rate $R(\langle\eta\rangle)$ at the cost of reducing the available signals $\int_{\eta_{\rm TH}}^1 p_{\eta_0,\sigma}(\eta)d\eta$. The authors of Ref. [26] showed that an optimal threshold η_T can be predetermined and the resulting key generation rate (4) can closely approach the ideal rate of Eq. (2) by making two key observations. First, there exists a critical transmittance $\eta_{\rm CR}$ such that $R(\eta) = 0$, for $\eta < \eta_{\rm CR}$. Thus, we have

$$R_{\max} = \int_0^1 R(\eta) p_{\eta_0,\sigma}(\eta)d\eta = \int_{\eta_{\rm CR}}^1 R(\eta) p_{\eta_0,\sigma}(\eta)d\eta. \tag{5}$$

Second, the rate $R(\eta)$, although convex in general, approaches linearity very well. Approximating the rate $R(\eta)$ as linear, $R(\eta) \approx \alpha\eta + \beta$, we have

$$\begin{aligned} R_{\max} &= \int_{\eta_{CR}}^1 R(\eta) p_{\eta_0,\sigma}(\eta)d\eta \\ &\approx \int_{\eta_{\rm CR}}^1 \alpha\eta p_{\eta_0,\sigma}(\eta)d\eta + \int_{\eta_{\rm CR}}^1 \beta p_{\eta_0,\sigma}(\eta)d\eta \\ &= R(\langle\eta\rangle) \times \int_{\eta_{\rm CR}}^1 p_{\eta_0,\sigma}(\eta)d\eta. \end{aligned} \tag{6}$$

This implies that by setting our threshold to the critical value, $\eta_{\rm TH} = \eta_{\rm CR}$, in Eq. (4), we achieve a very good approximation of $R_{\max}$. Importantly, the optimal transmittance cutoff does not depend on the channel's transmittance parameters, $\{\eta_0, \sigma\}$.

2. *Finite-size effects*

Taking the finite-size effects into consideration, the extracted secure key rate $R_{\text{finite-size}}$ also depends on the number of pulses N sent by Alice. Discarding low-transmittance events reduces the available postselected pulses to $N_{\rm post} = N \times \int_{\eta_{\rm TH}}^1 p_{\eta_0,\sigma}(\eta)d\eta$, so the distilled secure key rate is modified to [26]

$$R = R_{\text{finite-size}}(\langle\eta\rangle, N_{\rm post}) \times \int_{\eta_{\rm TH}}^1 p_{\eta_0,\sigma}(\eta)d\eta. \tag{7}$$

The rate $R_{\text{finite-size}}$ is calculated as

$$R_{\text{finite-size}} = \frac{\ell}{N}, \tag{8}$$

where ℓ is the number of distilled secure bits. The latter is found from

$$\ell = s_{X,0} + s_{X,1} - s_{\rm PA}(\phi_X) - s_{\rm EC}(e_{\rm obs}), \tag{9}$$

where $s_{X,0}$ and $s_{X,1}$ are the contributions from zero and single photon pulses, respectively, and $s_{\rm EC}$ and $s_{\rm PA}$ are the bits consumed to perform error correction and privacy amplification. The contributions $s_{X,0}$ and $s_{X,1}$, as well as the phase error ϕ_X, are estimated using the two-decoy-state method [42] adapted to include finite-size effects, according to Lim *et al.* [31]. The observed error $e_{\rm obs}$ is measured directly. Details of the secure key rate calculation are presented in Sec. IV.

The dependence of the rate $R_{\text{finite-size}}$ given by Eq. (8) on the number of sent pulses, N, raises the question of whether the main conclusion of the P-RTS method, i.e., that the optimum transmittance threshold can be predetermined independently of the channel statistics, still holds for the case of a finite number of sent pulses. Although the form of the distilled bits, ℓ [Eqs. (9) above and (10) in Sec. IV], does not allow us to easily examine it analytically, we were able to draw conclusions from numerical simulations.

The simulation results are presented in Fig. 1 for the parameters presented in Tables I and II. The examined

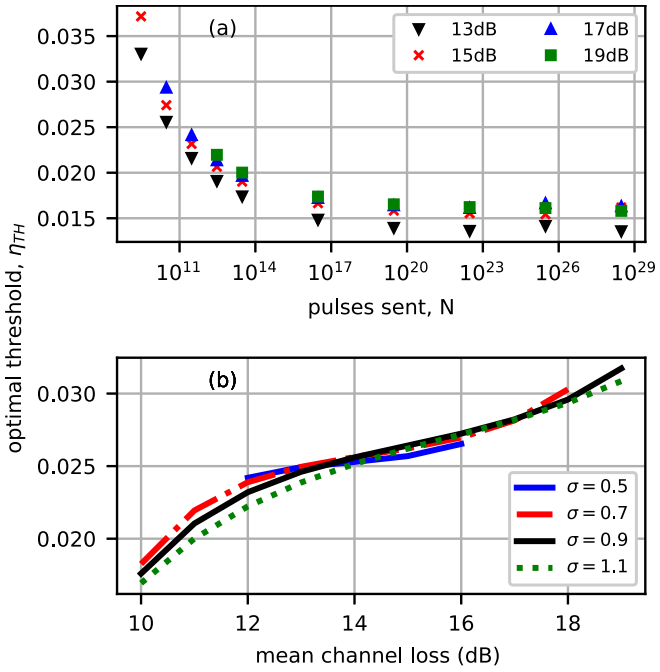

FIG. 1. Simulations. (a) The optimal transmittance threshold, for different number of sent pulses N and for different mean channel losses. Here, $\sigma = 0.9$ for all simulation points. (b) The optimum threshold in terms of the mean channel loss for different σ values. Here, $N = 3 \times 10^{10}$ for all simulation points.

TABLE I. Background-noise parameters for each detector. The input states have the same average photon number as the optimized states given in Table III. The background-click probability is given by $P_{\text{bg}}(\eta) = Y_0 + b\eta$.

	Y_0	b
Detector H	$(7.6 \pm 0.6) \times 10^{-6}$	$(2.6 \pm 0.4) \times 10^{-4}$
Detector V	$(3.1 \pm 0.2) \times 10^{-5}$	$(1.8 \pm 0.4) \times 10^{-4}$
Detector D	$(6.7 \pm 0.3) \times 10^{-5}$	$(2.7 \pm 0.4) \times 10^{-4}$
Detector A	$(6.7 \pm 0.3) \times 10^{-5}$	$(1.8 \pm 0.4) \times 10^{-4}$

channel-loss range (10–20 dB) is the range of most significance for the selection method given our detection parameters. For losses below this range, the selection method offers no significant improvement, while at greater losses, the extracted key rate is still insignificant or zero. The examined σ range (0.5–1.1) corresponds to typical values found in the literature [20,21,25].

Considering that for a realistic application of communication time of a few minutes at frequency 1 GHz, we can send $\sim 10^{11}$–10^{12} pulses, we observe that the optimum threshold at a low number of sent pulses, N, may differ from its asymptotic value. We also observe a similar variation on the optimum threshold for different values of the channel's parameters η_0 and σ. Moreover, this variation does not affect the secure key generation significantly. Given these observations, we conclude that even with an imperfect knowledge of the channel statistics, we can predetermine a transmittance cutoff which produces a near-optimum key generation rate. We explore this conclusion experimentally in Sec. IV.

TABLE II. Experiment parameters.

Bob's optical efficiency	0.42 ± 0.02
Optical misalignment	0.003 ± 0.002
Quantum efficiency (all detectors)	0.1 ± 0.05
Dead time	9 μs
f_{EC}	1.16
N	3×10^{10}

III. EXPERIMENTAL SETUP

The experimental setup is shown in Fig. 2. A continuous-wave (cw) laser source (Wavelength References) at 1550.5 nm (ITU channel 33.5) is directed to a $LiNbO_3$ (EOSPACE) intensity modulator (IM) to carve out pulses of full width at half maximum (FWHM) $\sim$2 ns at a 25-MHz repetition rate. The intensity modulator is driven by an arbitrary function generator (AFG) (Tektronix) with a sequence of three different voltage scales, implementing the three-decoy- (signal, weak, vacuum) state method. The DC bias voltage of the IM is automatically adjusted by a null point controller (PlugTech) to achieve the optimal extinction ratio (typically $\sim$30 dB). For each experimental session, Alice prepares and

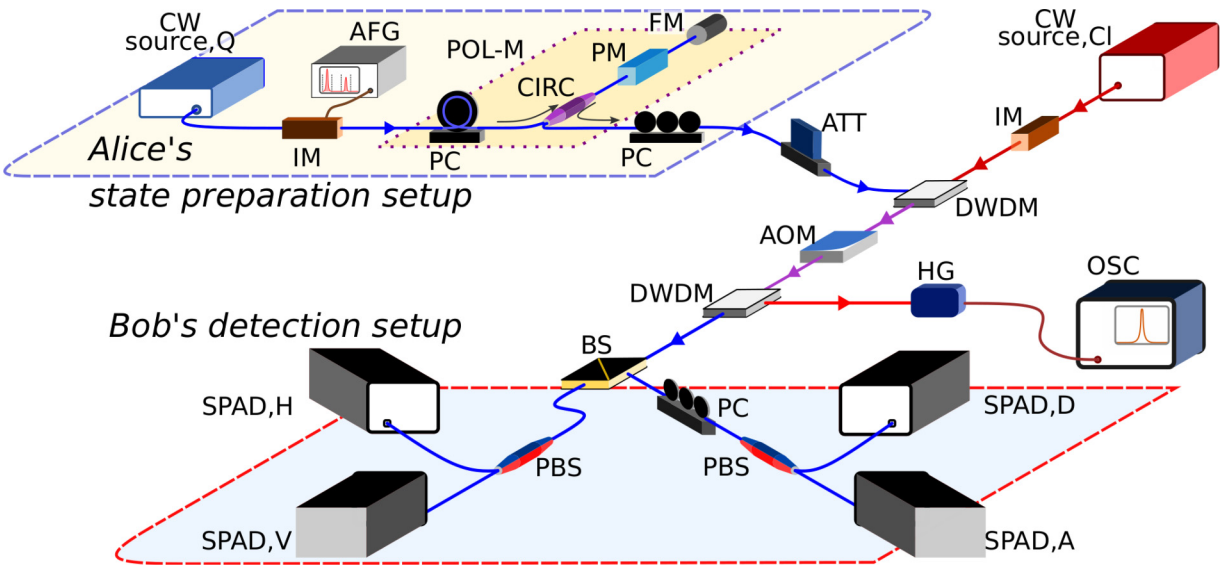

FIG. 2. A continuous-wave source (CW source, Q) is used to encode the quantum states on. Pulses are carved with an intensity modulator (IM) driven by an arbitrary function generator (AFG). The driving voltage sequence contains three voltage scales, implementing the three-decoy- (signal-weak-vacuum) state method. Bits are encoded as polarization states with a polarization modulation (POL-M) setup consisting of a polarization controller (PC), circulator (CIRC), phase modulator (PM), and Faraday mirror (FM). A polarization controller is used to align to the rectilinear basis. The beam is attenuated (ATT) to the desired photon number. An additional laser source (CW source, Cl) with an intensity modulator produces classical pulses that probe the channel statistics. The classical and quantum pulses are multiplexed at a dense wavelength division multiplexer (DWDM). Turbulence is simulated at an acousto-optic modulator (AOM). At Bob's side, a DWDM separates the classical and quantum signals. The high-intensity classical beam is read by a high-gain (HG) detector and sampled by an oscilloscope (OSC). The quantum beam is sent through a beam splitter (BS) to randomly select the measurement basis. Each polarization, i.e., horizontal, vertical, diagonal, antidiagonal (H,V,D,A), measurement is realized by a polarization beam splitter (PBS) and a single-photon avalanche detector (SPAD). An additional polarization controller is used to align to the diagonal (D) basis.

sends $N = 3 \times 10^{10}$ pulses. To implement polarization encoding BB84, we developed a fiber-based high-speed polarization modulator, following the design described in [43] which was proposed in [44].

The pulses are attenuated by a combination of digital and analog variable attenuators to single-photon levels. The pulses carrying the quantum states are multiplexed on a dense wavelength division multiplexer (DWDM) (Lightel) with 1554-nm (ITU channel 29) classical laser pulses at 4-kHz repetition rate and ∼3-ns FWHM. The classical pulses are used to probe the channel's transmittance statistics. Both sets of pulses are directed to an AOM (Brimrose), which is used to generate the random transmittance fluctuations expected from our turbulent channel. Another DWDM is employed at the receiver to separate the classical probe light and the quantum signals. The classical laser is detected by a high-gain detector (Thorlabs), and an oscilloscope (Tektronix) is used to sample and store the outputs of the detector. A 50:50 beam splitter (BS) is used to passively select Bob's detection basis, rectilinear or diagonal. Measurement in each basis is realized by a polarizing beam splitter (PBS) and a pair of InGaAs single-photon avalanche detectors (SPADs) (IDQ) gated at 25 MHz with ∼5-ns gate width.

The detector dead time is set to 9 μs to reduce the afterpulse probability. Since the afterpulse probability depends on the light intensity received by the detectors, we observe a linear dependence of the background probability P_{bg} in terms of the channel transmittance η of the form $P_{\text{bg}}(\eta) = Y_0 + b\eta$. The parameters Y_0 and b are extracted experimentally with linear fits from test measurements and are displayed in Table I using input light with the same average photon number as that used in the experiments.

The optical misalignment is approximately 3×10^{-3}. Each SPAD is set to 10% quantum efficiency (η_d). The experimental parameters are summarized in Table II. Bob's optical efficiency (η_{BOB}) refers to losses due to optical components (i.e., BS, PBS, and the fiber links). The output of each SPAD is recorded by a time-interval analyzer (TIA) (IDQ) and a custom-made program sifts them to collect the sets nX_k, mX_k, nZ_k, mZ_k, for $k \in \{\mu_1, \mu_2, \mu_3\}$, which are needed for the secure key distillation parameters according to the model of [31]. Here, nB_k are the detections where both Alice and Bob use the same basis $B \in \{X, Z\}$ while the decoy intensity k is used, and mB_k are the detections in error for the basis B and decoy intensity k.

Given the experimental parameters in Tables I and II, we numerically optimize the key generation to find the optimal parameters $\{q_X, P_{\mu_1}, P_{\mu_2}, \mu_1, \mu_2\}$. Here, q_X is the probability of using the rectilinear basis, P_{μ_1} and P_{μ_2} are the proportions of the signals and weak decoys, and μ_1, μ_2 are the signal and weak decoy intensities for the desired turbulence parameter set $\{\eta_0, \sigma\}$. The vacuum decoy parameters are fixed as $P_{\mu_3} = 1 - P_{\mu_1} - P_{\mu_2}$, and $\mu_3 = 0.002$. The optimized states are presented in Table III and the details of the optimization routine are presented in Appendix A.

IV. ANALYSIS AND RESULTS

Having collected all the sets nX_k, mX_k, nZ_k, mZ_k defined in the previous section for $k \in \{\mu_1, \mu_2, \mu_3\}$, we distill, according to [31], a secure key of length ℓ,

$$\ell = \left\lfloor s_{X,0} + s_{X,1}[1 - h(\phi_X)] - n_X f_{\text{EC}} h(e_{\text{obs}}) - 6\log_2\frac{21}{\varepsilon_{\text{sec}}} - \log_2\frac{2}{\varepsilon_{\text{cor}}} \right\rfloor, \quad (10)$$

where $s_{X,0}$ and $s_{X,1}$ are the lower bounds on the number of bits generated by zero- and single-photon pulses (which are immune to photon number splitting attacks) while both Alice and Bob use the rectilinear basis, ϕ_X is the upper bound on the phase error, $h(\cdot)$ is the binary entropy function,

$$h(x) = -x\log_2 x - (1-x)\log_2(1-x), \quad (11)$$

and $e_{\text{obs}} = \frac{m_X}{n_X}$ is the quantum bit error rate, with $m_X = mX_{\mu_1} + mX_{\mu_2} + mX_{\mu_3}$ and $n_X = nX_{\mu_1} + nX_{\mu_2} + nX_{\mu_3}$. The term $-n_X f_{\text{EC}} h(e_{\text{obs}})$ describes the bits consumed by the classical error-correction algorithm [45] with efficiency $f_{\text{EC}} = 1.16$, and $\varepsilon_{\text{cor}} = 10^{-15}$ is the correctness parameter. The term $-s_{X,1}h(\phi_X)$ describes the bits consumed during the privacy amplification stage to achieve secrecy according to the secrecy parameter $\varepsilon_{\text{sec}} = 10^{-10}$.

We explore the premise of Sec. II, whereby one can predetermine a near-optimal transmittance cutoff while considering finite-size effects, even with an imperfect knowledge of the channel statistics. For each examined channel loss (11–19 dB), Alice prepares her state parameters while (i) having perfect knowledge of the channel, (ii) underestimating the mean loss by 2 dB, and (iii) overestimating the mean loss by 2 dB. For example, at the 17 dB mean channel loss, Alice assumes (i) 17, (ii) 15, and (iii) 19 dB mean channel loss and prepares her state (Table III) accordingly. A 2-dB uncertainty window for the mean channel loss can be comfortably achieved by classical means during the initial calibration stage. In any case, such knowledge of the channel parameters is required and should be pursued for the construction of Alice's state (Table III) as the state parameters (especially the proportions $\{q_X, P_{\mu_1}, P_{\mu_2}\}$) are sensitive to the mean channel loss. For this reason, we did not consider the case of larger uncertainty on the channel loss.

We present our measurement results in Fig. 3 for each channel loss and optimized state. The measurement data points correspond to ARTS [25]-type postselection, where we scan successive transmittance cutoffs and extract the corresponding secure key rate. The yellow shaded area corresponds to the variance on the optimal cutoff observed in Fig. 1. The error bars represent an uncertainty ±0.005 in setting, during the experiment, the desired signal photon number μ_1 and weak decoy photon number μ_2 given in Table III. In

TABLE III. Alice's optimized quantum states, for channel parameters $\sigma = 0.9$ and mean channel loss 11, 13, 15, 17, and 19 dB.

Turbulence	q_x	P_{μ_1}	P_{μ_2}	μ_1	μ_2
$\{\eta_0 = 10^{-1.1},\ \sigma = 0.9\}$	0.904	0.660	0.215	0.56	0.225
$\{\eta_0 = 10^{-1.3},\ \sigma = 0.9\}$	0.879	0.617	0.244	0.56	0.23
$\{\eta_0 = 10^{-1.5},\ \sigma = 0.9\}$	0.844	0.552	0.287	0.56	0.23
$\{\eta_0 = 10^{-1.7},\ \sigma = 0.9\}$	0.789	0.460	0.352	0.54	0.24
$\{\eta_0 = 10^{-1.9},\ \sigma = 0.9\}$	0.683	0.319	0.439	0.54	0.245

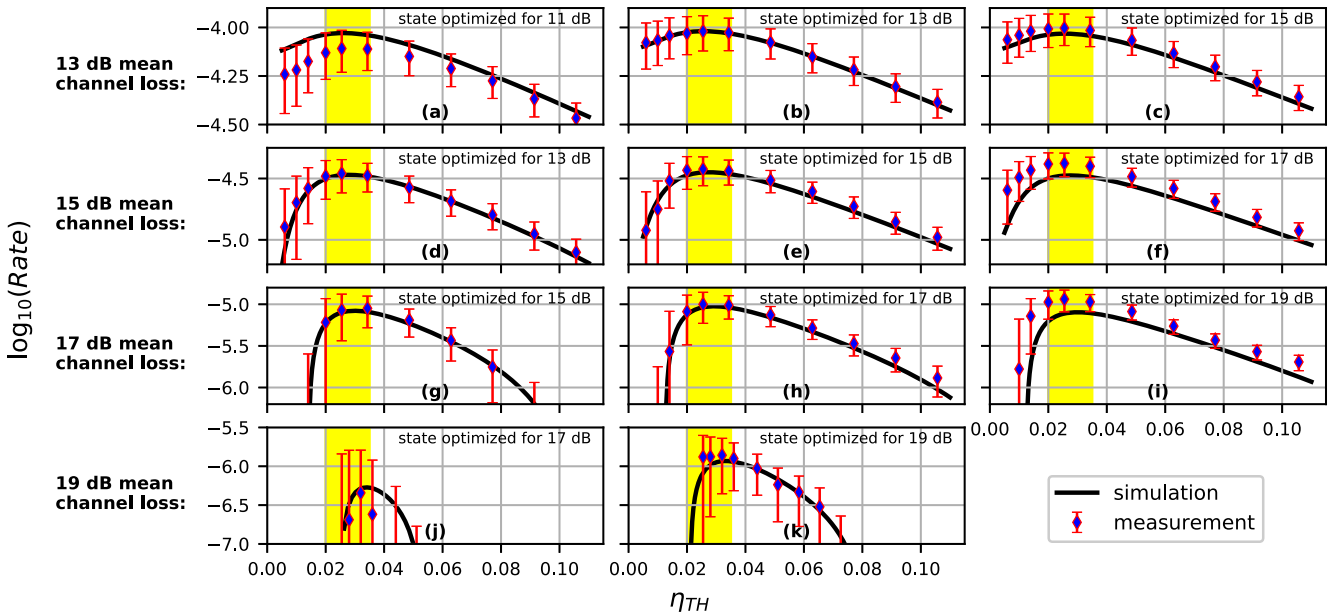

FIG. 3. ARTS-type measurements: The logarithm of the secure key rate for increasing applied transmittance cutoff. (a)–(c) Distilled secure key rates at 13 dB mean channel loss for increasing applied transmittance cutoffs. Alice optimizes her state assuming (a) 11, (b) 13, and (c) 15 dB mean channel loss. (d)–(f) Similar for 15 dB channel loss, and (d) 13, (e) 15, and (f) 17 dB loss assumed by Alice. (g)–(i) Similar for 17 dB channel loss, and (d) 15, (e) 17, and (f) 19 dB loss assumed by Alice. (j),(k): 19 dB channel loss, and (j) 17 and (k) 19 dB loss assumed by Alice; no key is generated if Alice assumes 21 dB loss. The error bars represent a ± 0.005 uncertainty in the signal and weak decoy average photon number. The yellow shaded areas represent the range of variation on the optimal transmittance threshold, presented in Fig. 1.

practical applications though, intensity uncertainties should be treated more formally with methods such as those discussed in Ref. [46].

We observe that for a wide range of mean channel losses (13–17 dB) and within the range of uncertainty of the optimal threshold (yellow shaded range), the extracted secure key rate does not vary significantly from its optimal value. However, this conclusion does not hold well at higher losses, where more precise knowledge of the channel parameters is required, in order to both prepare Alice's state parameters and apply the selection threshold.

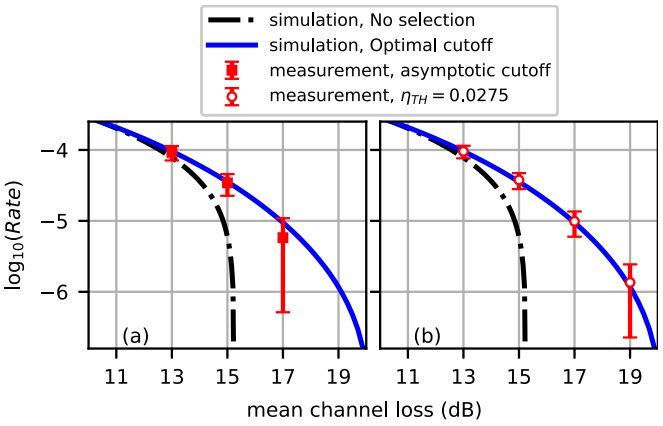

FIG. 4. P-RTS-type measurements. (a) Cutoff set as $\eta_{\mathrm{TH}} = 0.016$, i.e., the asymptotic optimal cutoff. This cutoff does not generate a key at 19 dB mean channel loss. (b) Cutoff set as $\eta_{\mathrm{TH}} = 0.0275$, i.e., an average cutoff observed in Fig. 1.

In Fig. 4, we present an evaluation of our P-RTS-type measurements where a fixed and predetermined cutoff transmittance is set. In Fig. 1(a), we have observed that the optimal threshold approaches the value $\eta_{\mathrm{TH}} = 0.016$ as the number of sent pulses, N, becomes large. We acquire a similar value from the root of the equation $R_{\mathrm{GLLP}}(\eta) = 0$, where $R_{\mathrm{GLLP}}(\eta)$ is the Gottesman-Lo-Lutkenhaus-Preskill (GLLP) [47] asymptotic secure key rate as a function of the channel transmittance. This value is the asymptotic cutoff applied in Fig. 4(a) and it can be predetermined without any knowledge of the channel statistics [26]. In Fig. 1(b), we have observed a limited variance in the optimal threshold around the value $\eta_{\mathrm{TH}} = 0.0275$ throughout the range of channel parameters where the selection method offers significant improvement on the extracted key rate. We choose this value to represent a threshold acquired through partial knowledge of the channel parameters.

Figure 4 shows that for a wide range of the examined mean channel loss, the asymptotic threshold only slightly underperforms the threshold acquired through partial knowledge of the channel. However, at higher losses, a P-RTS-type (channel-independent) threshold fails to produce a secure key rate and some partial knowledge of the channel parameters is required. In any case, choosing the asymptotic threshold still allows ARTS-type scanning during postselection to fully maximize the generated secure key rate.

V. CONCLUDING REMARKS

We conducted an experimental demonstration of decoy-state BB84 QKD over a simulated turbulent channel taking finite-size effects into account. We showed that the main conclusion of the prefixed-threshold real-time selection (P-RTS) scheme proposed in [26], where the transmittance threshold

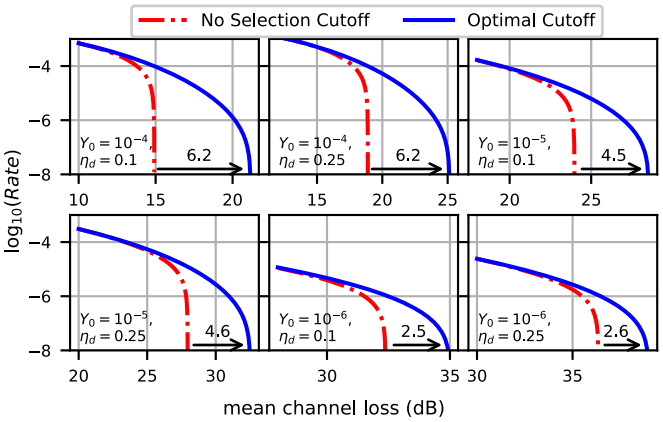

FIG. 5. Simulations: The improvement that the selection method offers for typical SPAD background (Y_0) and quantum efficiency (η_d) values. As a comparison criterion, we examine the mean channel loss at which a key rate of 10^{-8} can be achieved. Sample size is $N = 3 \times 10^{10}$ and the optimal cutoff is applied. $\sigma = 0.9$.

can be predetermined independently of the channel statistics, holds well in the regime of realistically finite events, further supporting the applicability of the method. The secure key rate can be significantly improved in turbulent atmospheric conditions, especially at high loss. The selection method can be easily implemented without any significant technological upgrades, while saving computational resources. We observe that it is especially beneficial for lower-quality detection setups, with higher detection noise, as the turbulence impacts their SNR more severely. We offer supporting simulations in Fig. 5. For example, by applying a transmittance cutoff at background noise $Y_0 = 10^{-4}$, we can extend the mean channel loss so that a 10^{-8} key rate is generated by 6.2 dB. For $Y_0 = 10^{-6}$, this extension is for 2.5 dB.

Depending on the knowledge of the turbulence statistics, the two selection methods could be used in combination. One could select a conservative transmittance threshold to perform P-RTS-type real-time data rejection and then perform an ARTS-type scan during postselection to further maximize the extracted secure key rate.

It should be pointed out that one important assumption behind the security proof adopted in this work is that the global phase of Alice's quantum state signal is random [48]. This could be achieved by using a PM at Alice's station to actively randomize the phase of each quantum signal, as demonstrated in [49]. For simplicity, we did not implement phase randomization. Nevertheless, since the coherence time of Alice's laser is much smaller than the data-collection time, the detection statistics observed in our experiment match the case where phase randomization is applied.

A similar technique could be used to enhance free-space MDI QKD, as well as other free-space protocols where the secure key rate can be approximated as a straight line at the lower boundary. Being able to overcome the challenges of atmospheric turbulence is a crucial step in building a future global quantum network.

ACKNOWLEDGMENTS

This work was supported by the U.S. Office of Naval Research under Award No. N00014-15-1-2646. We thank H.-K. Lo and W. Wang for useful comments, and Raphael Pooser for help with the initial setup. B.Q. acknowledges support from the U.S. Department of Energy (DOE) Office of Cybersecurity Energy Security and Emergency Response (CESER) through the Cybersecurity for Energy Delivery Systems (CEDS) program.

APPENDIX A: OPTIMIZING THE SECURE KEY RATE

Decoy-state QKD introduces additional degrees of freedom for the pulses that are sent. Optimization of these parameters can have a profound effect on the secure key rate. In this Appendix, we explain how the secure key rate is calculated and describe the optimization process. We assume that Alice has full knowledge of Bob's detection setup parameters, as summarized in Table II. She knows that Bob will apply a selection threshold and she also has some knowledge of the channel parameters $\{\eta_0, \sigma\}$, according to the discussion in Sec. IV. For the rest of the section, we follow the notation of Lim *et al.* [31], where X denotes the rectilinear (computational) basis and Z the diagonal (Hadamard) basis. Alice performs a numerical optimization over the free parameters of her state, $\{q_X, P_{\mu_1}, P_{\mu_2}, \mu_1, \mu_2\}$, where q_X is the fraction of bits encoded in the X basis, P_{μ_1} and P_{μ_2} are the fractions of the signal state and weak decoy-state bits, respectively, and μ_1 and μ_2 are the photon numbers per pulse for the signal and weak decoy states, respectively. For the vacuum decoy state, we have fixed $\mu_3 = 0.002$, and $P_{\mu_3} = 1 - P_{\mu_1} - P_{\mu_2}$.

The detection probability for the decoy $k \in \{\text{signal, weak, vacuum}\}$ at the detector measuring the i polarization state, where $i \in \{H, V, D, A\}$, is

$$P^i_{\text{click}}(\mu_k) = 1 - \left(1 - p^i_{\text{bg}}\right) e^{-\eta^i_{\text{SYS}}\mu_k}. \tag{A1}$$

The error probability is

$$E^i(\mu_k) = 1 - \left(1 - p^{\perp i}_{\text{bg}}\right) e^{-e_{\text{mis}}\eta^{\perp i}_{\text{SYS}}\mu_k}, \tag{A2}$$

where $\eta^i_{\text{SYS}} = \eta \times \eta_{\text{BOB}} \times \eta_d$ is the total transmission leading to detector i [i.e., the channel transmittance (η), the transmittance of Bob's optical instruments (η_{BOB}), and the detector's quantum efficiency (η_d)]. In Eq. (A2), $p^{\perp i}_{\text{bg}}$ is the background noise probability on the detector orthogonal to i and e_{mis} is the optical misalignment. We note that the background-noise probability is taken as a linear function of the channel's transmittance η: $p_{\text{bg}} = p_{\text{bg}}(\eta) = Y_0 + b\eta$.

The numerical optimization returns the parameters $\{q_X, P_{\mu_1}, P_{\mu_2}, \mu_1, \mu_2\}$ that maximize the secure key rate $R = \frac{\ell}{N}$ for a given number N of sent pulses ($N = 3 \times 10^{10}$ for our experiment), where ℓ is the number of distilled bits [31],

$$\ell = \Big\lfloor s_{X,0} + s_{X,1}[1 - h(\phi_X)] - n_X f_{\text{EC}} h(e_{\text{obs}}) - 6\log_2\frac{21}{\varepsilon_{\text{sec}}} - \log_2\frac{2}{\varepsilon_{\text{cor}}} \Big\rfloor. \tag{A3}$$

To summarize the approach of Lim *et al.* in [31], we estimate the lower bound of the zero-photon pulse's contribution as

$$s_{X,0} \geqslant \tau_0 \frac{\mu_2 n^-_{X,\mu_3} - \mu_3 n^+_{X,\mu_2}}{\mu_2 - \mu_3}, \tag{A4}$$

and the lower bound of the single-photon pulse's contribution as

$$s_{X,1} \geqslant \frac{\tau_1\mu_1\left[n^-_{X,\mu_2} - n^+_{X,\mu_3} - \frac{\mu_2^2-\mu_3^2}{\mu_3^2}\left(n^+_{X,\mu_1} - \frac{s_{X,0}}{\tau_0}\right)\right]}{\mu_1(\mu_2-\mu_3)-\mu_2^2+\mu_3^2}. \quad \text{(A5)}$$

In the above, we use the conditional probability τ_n that an n-photon pulse is sent,

$$\tau_n = \sum_k \frac{e^{-k}k^n p_k}{n!}, \quad \text{(A6)}$$

and $n^{\pm}_{X,k}$ the number of detections where both Alice and Bob use the X basis, considering the finite sample size:

$$n^{\pm}_{X,k} := \frac{e^k}{p_{\mu_k}}\left[n_{X,k} \pm \sqrt{\frac{n_X}{2}\ln\frac{21}{\varepsilon_{\text{sec}}}}\right]. \quad \text{(A7)}$$

The detection numbers $n_{X,k}$ are calculated from Eqs. (A1) and (A2). Here, $n_X = n_{X,\mu_1} + n_{X,\mu_2} + n_{X,\mu_3}$. The observed error in the rectilinear basis, e_{obs}, is calculated as $e_{\text{obs}} = \frac{m_X}{n_X}$ with $m_X = m_{X,\mu_1} + m_{X,\mu_2} + m_{X,\mu_3}$. The numbers of errors, $m_{X,k}$, is calculated from Eq. (A2). Similar expressions hold in the diagonal basis by replacing $X \to Z$.

We estimate the upper bound of the phase error rate as

$$\phi_X \leqslant \frac{v_{Z,1}}{s_{Z,1}} + \gamma\left(\epsilon_{\text{sec}}, \frac{v_{Z,1}}{s_{Z,1}}, s_{Z,1}, s_{X,1}\right). \quad \text{(A8)}$$

Here, $\gamma(\cdot)$ is the estimation uncertainty and $v_{Z,1}$ is the number of errors stemming from single-photon pulses in the diagonal basis and is estimated as

$$v_{Z,1} \leqslant \tau_1\frac{\mu_2 m^+_{Z,\mu_2} - \mu_3 m^-_{Z,\mu_3}}{\mu_2-\mu_3}, \quad \text{(A9)}$$

with $m^{\pm}_{Z,k}$ the number of errors in the diagonal basis considering the finite sample size,

$$m^{\pm}_{Z,k} := \frac{e^k}{p_{\mu_k}}\left[m_{Z,k} \pm \sqrt{\frac{m_Z}{2}\ln\frac{21}{\varepsilon_{\text{sec}}}}\right]. \quad \text{(A10)}$$

APPENDIX B: ESTIMATING THE CHANNEL'S TRANSMITTANCE WITH CLASSICAL PROBE PULSES

In our experiment, classical probe pulses at a 4-kHz repetition rate and ~3 ns FWHM at the 29 ITU channel are sent along the quantum pulses. After passing the AOM, they are separated from the quantum pulses with a DWDM and collected by a high-gain classical photodetector. We utilize the fast-frame feature of a DPO 7205 Tektronix Oscilloscope, which stores samples in a short interval around the trigger [16 ns in Fig. 6(b) sampled at 5 G-samples/sec]. Thus, we acquire high-resolution pulses [Fig. 6(b)] with minimum data storage. By performing a Gaussian fit on the pulses, we acquire the area under each pulse, which is a direct measure of the transmitted intensity. For an initial calibration set, we correlate, with a polynomial fit, the measured pulse area with the programmed transmittance. For the actual measurements, we use this polynomial fit to deduce the transmittance given the measured pulse area. We note that we achieve similar resolution in Fig. 6(a) by simply calculating the sum of the samples of each frame, which is also significantly faster to compute compared to the Gaussian fits.

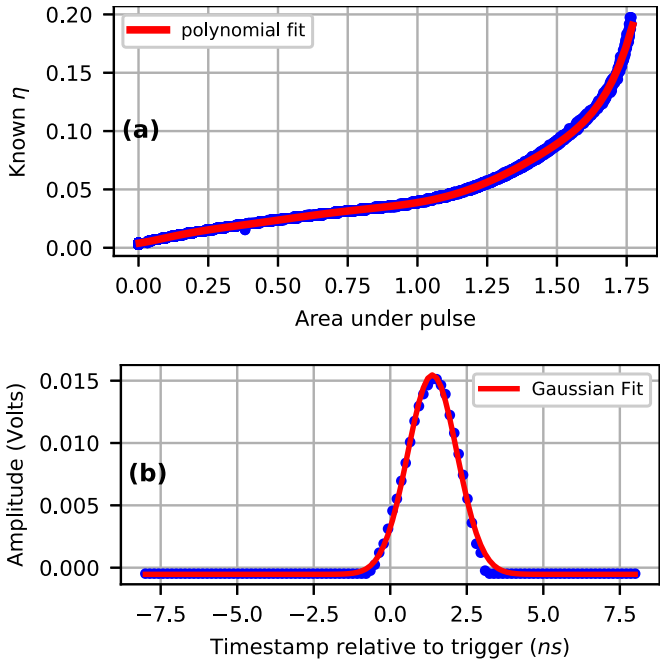

FIG. 6. (a) Polynomial fit to determine the correlation between the measured area under the probe pulse and the programmed transmittance. (b) Example of a probed pulse captured by the oscilloscope and its Gaussian fit.

[1] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai *et al.*, Opt. Express **19**, 10387 (2011).

[2] Y.-L. Tang, H.-L. Yin, Q. Zhao, H. Liu, X.-X. Sun, M.-Q. Huang, W.-J. Zhang, S.-J. Chen, L. Zhang, L.-X. You, Z. Wang, Y. Liu, C.-Y. Lu, X. Jiang, X. Ma, Q. Zhang, T.-Y. Chen, and J.-W. Pan, Phys. Rev. X **6**, 011024 (2016).

[3] C. Simon, Nat. Photon. **11**, 678 (2017).

[4] W. K. Wootters and W. H. Zurek, Nature (London) **299**, 802 (1982).

[5] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998).

[6] C. J. Pugh, S. Kaiser, J.-P. Bourgoin, J. Jin, N. Sultana, S. Agne, E. Anisimova, V. Makarov, E. Choi, B. L. Higgins *et al.*, Quantum Sci. Technol. **2**, 024009 (2017).

[7] S. Nauerth, F. Moll, M. Rau, C. Fuchs, J. Horwath, S. Frick, and H. Weinfurter, Nat. Photon. **7**, 382 (2013).

[8] J.-Y. Wang, B. Yang, S.-K. Liao, L. Zhang, Q. Shen, X.-F. Hu, J.-C. Wu, S.-J. Yang, H. Jiang, Y.-L. Tang, B. Zhong, H. Liang, W.-Y. Liu, Y.-H. Hu, Y.-M. Huang, B. Qi, J.-G. Ren, G.-S. Pan, J. Yin, J.-J. Jia *et al.*, Nat. Photon. **7**, 387 (2013).

[9] H.-Y. Liu, X.-H. Tian, C. Gu, P. Fan, X. Ni, R. Yang, J.-N. Zhang, M. Hu, Y. Niu, X. Cao, X. Hu, G. Zhao, Y.-Q. Lu, Z. Xie, Y.-X. Gong, and S.-N. Zhu, Natl. Sci. Rev. **7**, 921 (2020).

[10] J. G. Rarity, P. R. Tapster, P. M. Gorman, and P. Knight, New J. Phys. **4**, 82 (2002).

[11] E. Meyer-Scott, Z. Yan, A. MacDonald, J.-P. Bourgoin, H. Hübel, and T. Jennewein, Phys. Rev. A **84**, 062326 (2011).

[12] G. Vallone, D. Bacco, D. Dequal, S. Gaiarin, V. Luceri, G. Bianco, and P. Villoresi, Phys. Rev. Lett. **115**, 040502 (2015).

[13] S.-K. Liao, H.-L. Yong, C. Liu, G.-L. Shentu, D.-D. Li, J. Lin, H. Dai, S.-Q. Zhao, B. Li, J.-Y. Guan, W. Chen, Y.-H. Gong, Y. Li, Z.-H. Lin, G.-S. Pan, J. S. Pelc, M. M. Fejer, W.-Z. Zhang, W.-Y. Liu, J. Yin, J.-G. Ren *et al.*, Nat. Photon. **11**, 509 (2017).

[14] 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).

[15] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, F.-Z. Li, J.-F. Wang, Y.-M. Huang, L. Deng, T. Xi, L. Ma, T. Hu *et al.*, Phys. Rev. Lett. **120**, 030501 (2018).

[16] J. Yin, Y.-H. Li, S.-K. Liao, M. Yang, Y. Cao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, S.-L. Li, R. Shu, Y.-M. Huang, L. Deng, L. Li, Q. Zhang, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, X.-B. Wang, F. Xu *et al.*, Nature (London) **582**, 501 (2020).

[17] D. Vasylyev, A. A. Semenov, and W. Vogel, Phys. Rev. Lett. **117**, 090501 (2016).

[18] D. Vasylyev, W. Vogel, and A. A. Semenov, Phys. Rev. A **97**, 063852 (2018).

[19] P. Diament and M. C. Teich, J. Opt. Soc. Am. **60**, 1489 (1970).

[20] P. W. Milonni, J. H. Carter, C. G. Peterson, and R. J. Hughes, J. Opt. B: Quantum Semiclassical Opt. **6**, S742 (2004).

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

[22] A. Al-Habash, L. C. Andrews, and R. L. Phillips, Opt. Engineer. **40**, 1554 (2001).

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

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

[25] 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).

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

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

[28] Z.-D. Zhu, D. Chen, S.-H. Zhao, Q.-H. Zhang, and J.-H. Xi, Quantum Inf. Proc. **18**, 33 (2018).

[29] W. Wang, F. Xu, and H.-K. Lo, Prefixed-threshold real-time selection for free-space measurement-device-independent quantum key distribution, arXiv:1910.10137.

[30] C. H. Bennett and G. Brassard, Theor. Comput. Sci. **560**, 7 (2014).

[31] Charles Ci Wen Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, Phys. Rev. A **89**, 022307 (2014).

[32] M. Bohmann, R. Kruse, J. Sperling, C. Silberhorn, and W. Vogel, Phys. Rev. A **95**, 063801 (2017).

[33] C. Rickenstorff, J. A. Rodrigo, and T. Alieva, Opt. Express **24**, 10000 (2016).

[34] F. Wang, I. Toselli, and O. Korotkova, Appl. Opt. **55**, 1112 (2016).

[35] P. Chaiwongkhot, K. B. Kuntz, Y. Zhang, A. Huang, J.-P. Bourgoin, S. Sajeed, N. Lütkenhaus, T. Jennewein, and V. Makarov, Phys. Rev. A **99**, 062315 (2019).

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

[37] S. Karp, R. M. Gagliardi, S. E. Moran, and L. B. Stotts, *Optical Channels: Fibers, Clouds, Water, and the Atmosphere* (Springer Science & Business Media, New York, 2013).

[38] J. W. Goodman, *Statistical Optics* (Wiley, New York, 2015).

[39] H. Smith, D. Dube, M. Gardner, S. Clough, and F. Kneizys, *FASCODE-Fast Atmospheric Signature Code (Spectral Transmittance and Radiance)*, Tech. Rep. No. 2 (Visidyne Inc., Burlington, MA, 1978).

[40] A. Berk, L. S. Bernstein, and D. C. Robertson, *MODTRAN: A Moderate Resolution Model for LOWTRAN*, Tech. Rep. No. SSI-TR-124 (Spectral Sciences Inc., Burlington, MA, 1987).

[41] 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 (Rev. 5) User's Manual (Spectral Sciences Inc., Burlington, MA, 2016).

[42] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Phys. Rev. A **72**, 012326 (2005).

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

[44] I. Lucio-Martinez, P. Chan, X. Mo, S. Hosier, and W. Tittel, New J. Phys. **11**, 95001 (2009).

[45] G. Brassard and L. Salvail, in *Advances in Cryptology — EUROCRYPT '93*, edited by T. Helleseth (Springer, Berlin, 1994), pp. 410–423.

[46] A. Mizutani, M. Curty, C. C. W. Lim, N. Imoto, and K. Tamaki, New J. Phys. **17**, 093011 (2015).

[47] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **5**, 325 (2004).

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

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