Genuine time-bin-encoded quantum key distribution over a turbulent depolarizing free-space channel

JEONGWAN JIN,[1,3] (iD) JEAN-PHILIPPE BOURGOIN,[1] RAMY TANNOUS,[1] SASCHA AGNE,[1] CHRISTOPHER J. PUGH,[1] KATANYA B. KUNTZ,[1] BRENDON L. HIGGINS,[1] AND THOMAS JENNEWEIN[1,2,4]

[1]*Institute for Quantum Computing, Department of Physics and Astronomy, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada*
[2]*Quantum Information Science Program, Canadian Institute for Advanced Research, Toronto, Ontario M5G 1Z8, Canada*
[3]*jeongwan.jin@nrc-cnrc.gc.ca*
[4]*thomas.jennewein@uwaterloo.ca*

Abstract: Despite its widespread use in fiber optics, encoding quantum information in photonic time-bin states is usually considered impractical for free-space quantum communication as turbulence-induced spatial distortion impedes the analysis of time-bin states at the receiver. Here, we demonstrate quantum key distribution using time-bin photonic states distorted by turbulence and depolarization during free-space transmission. Utilizing a novel analyzer apparatus, we observe stable quantum bit error ratios of 5.32 %, suitable for generating secure keys, despite significant wavefront distortions and polarization fluctuations across a 1.2 km channel. This shows the viability of time-bin quantum communication over long-distance free-space channels, which will simplify direct fiber/free-space interfaces and enable new approaches for practical free-space quantum communication over multi-mode, turbulent, or depolarizing channels.

1. Introduction

Networks of quantum information processors—a Quantum Internet—demand the reliable transmission of quantum bits between nodes via optical-fiber or free-space channels [1]. Encoding quantum information in photonic time-bin states is often preferred for realizing quantum-network components in optical fibers; e.g., boson sampling [2], optical-fiber quantum memory [3], city-wide quantum teleportation [4], and high-dimensional quantum key distribution (QKD) [5]. However, time-bin encoding is usually considered impractical in free space as conventional analyzers are hindered by the effects of atmospheric turbulence and steering-optics misalignment [6]. In fact, free-space quantum communication has been demonstrated by utilizing different degrees of freedom on various platforms, including polarization-encoded satellite QKD [7], orbital-angular-momentum-encoded high-dimensional QKD [8], and daylight QKD with integrated chips [9]. Hyper-entanglement between energy-time and polarization has also been distributed across 1.2 km free-space link [10].

Practical time-bin encodings of quantum bits (qubits) must have a sufficiently large temporal separation between *early* and *late* time-bins that optical pulses are easily distinguishable in the presence of system timing jitters—e.g., on the order of 1 ns for direct detection. This temporal separation defines the difference in lengths of the two paths of an asymmetric interferometer used to analyze the time-bin states. But, when given an optical mode that is spatially distorted by atmospheric turbulence, the evolutions of the spatial modes through each of those two paths will be significantly distinguishable [6]. Consequently, the interference contrast of superpositions of early and late time-bins is degraded. Spatial-mode filtering via coupling to single-mode fiber can

be used to avoid this problem, but doing so results in significant throughput loss for long distance links [11]. Wavefront corrections with adaptive optics can help, but is expensive and technically challenging [12,13]. Therefore, a purely passive multimodal optical solution is preferable.

Recent work has achieved significant progress on passive optical solutions. For instance, Jin *et al* showed two approaches of field-widened interferometers used as analyzers for a multi-mode photonic time-bin qubit entangled with a separate polarization qubit, proving the viability of time-bin encoding for quantum communication in multi-mode optical channels [6]. A similar concept was implemented by Vallone *et al*, who observed interference between two temporal modes of laser pulses which were attenuated to single-photon levels after being reflected by orbiting satellites [14]. Until now, however, a genuine time-bin-based quantum protocol over a long-distance atmospheric link has not been demonstrated.

Here, we demonstrate QKD between two separate parties using time-bin encoding as an alternative means for free-space quantum communication. First, we prepare time-bin quantum states, encoded in early and late time-bin with a 2-ns separation, and send them through a polarization-mixing channel before traveling 1.2 km of free-space atmosphere and becoming spatially distorted by turbulence. At the receiver, the polarization- and spatially-distorted photons are coupled into a step-index multi-mode fiber, which supports approximately 1870 propagating spatial modes [15]. The collected photons are directed to our multi-mode time-bin qubit decoder (MM-TQD) where passive mode-correcting optics ensure high quality of interference regardless of the spatial shape of the incoming photons.

2. Experiment

We implement the BB84 QKD protocol [16] with decoy states [17–19]. Our apparatus (Fig. 1) prepares time-bin qubits using 300-ps-long 785-nm-wavelength weak coherent pulses, with ≈ 0.5 mean photons per pulse, generated at a rate of 150 MHz. Although other wavelengths may be used, 785 nm is an excellent compromise for satellite-uplink long-distance QKD [20], while portable and room-temperature-operating single-photon detectors provide high detection efficiency. For information encoding, we use a time-bin qubit encoder (TQE) consisting of an unbalanced interferometer with path length difference matched to the MM-TQD. Where $|E\rangle$ and $|L\rangle$ represent early and late time-bins, respectively, the state $|E\rangle$, $|L\rangle$, $(|E\rangle + |L\rangle)/\sqrt{2}$, or $(|E\rangle - |L\rangle)/\sqrt{2}$ is encoded onto each pulse, following a randomized sequence. (See Appendix A for details.) The time-bin-encoded photon is then coupled into a single-mode fiber and guided to a 12-cm-diameter launch telescope.

After traversing the free-space channel located at the North Campus of the University of Waterloo, the single photons are captured by a 10-cm-diameter receiver telescope and collected in a multi-mode fiber which guides the light to our MM-TQD for projection measurements. The MM-TQD consists of an unbalanced interferometer with a matched pair of lenses in each path, minimizing relative dispersion. The focal lengths of each lens pair, $f_{\text{short path}} = 50$ mm and $f_{\text{long path}} = 200$ mm, are chosen such that the image of the incoming spatial mode at the input beam splitter is recovered at the output beam splitter after traversing each path of the interferometer, thus removing path distinguishability caused by path-length differences while maintaining the temporal separation between the paths. For an input multi-mode beam, we measure interference visibility of up to 97 %. Photons are collected into multi-mode fiber, with total throughput of 81 % from input to output, and are finally detected by silicon avalanche single-photon detectors (Si-SPDs). A QKD post-processing algorithm is applied to the data, including error correction and privacy amplification (see Appendix B), to produce secret key bits.

To characterize the channel, a separate ~100 µW 850-nm-wavelength laser is polarized and merged with the quantum signals via a single-mode beam combiner at the transmitter before entering the launch telescope. At the receiver, a portion of this light is captured by a complementary metal-oxide semiconductor (CMOS) sensor at a frame rate of 20 Hz for 60 s at
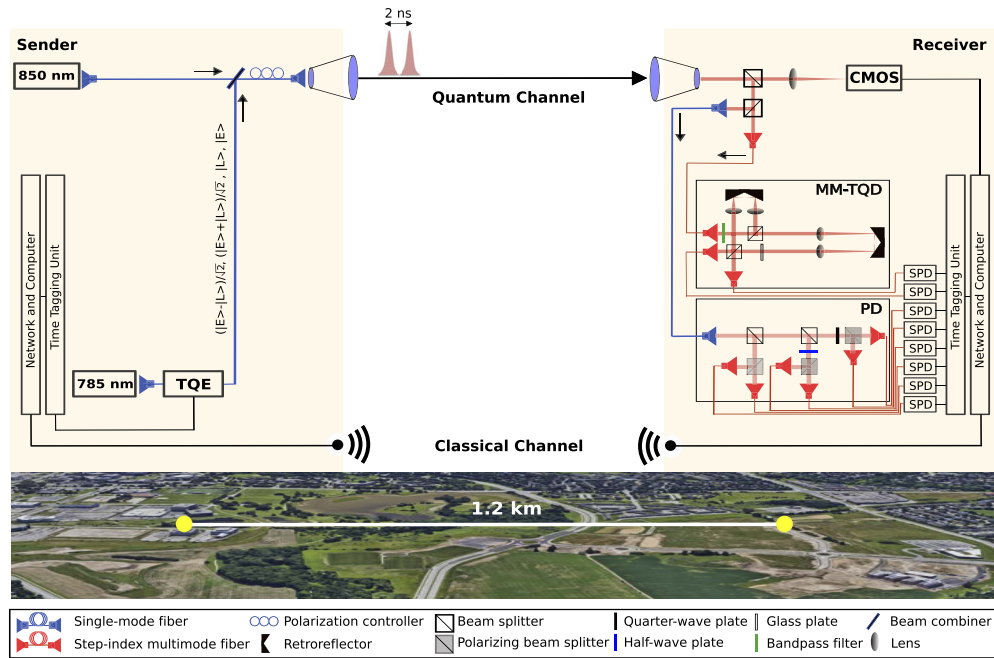
Fig. 1. Experimental setup. Time-bin photonic qubit states, $|E\rangle$, $|L\rangle$, $(|E\rangle + |L\rangle)/\sqrt{2}$, or $(|E\rangle - |L\rangle)/\sqrt{2}$, are generated in a time-bin qubit encoder (TQE). The signals traverse 1.2 km of atmosphere to the receiver, and are coupled via multi-mode fiber to time-bin qubit decoder (MM-TQD) for analysis. A separate laser beam at 850 nm co-propagates with time-bin-encoded photons, and is used to characterize the degree of turbulence and polarization mixture in the optical channel. A spatial image of this light is captured by the CMOS sensor, and its polarization state is analyzed by the 6-state polarization decoder (PD). All detected signals from single-photon detectors (SPDs) are sent to a time-tagging unit and a computer for data analysis. Classical communication is done through a radio-frequency local network channel.

a time, by which we assess beam distortions and spatial misalignment caused by the turbulent atmosphere. A portion of the laser beam is coupled into a single-mode fiber before undergoing tomographic polarization analysis [21]—consisting of 6-state projection and photon counting with Si-SPDs (see Appendix C)—to assess the polarization preservation of the channel. A bandpass filter centered at 785 nm is placed at the entrance of the MM-TQD to block 850-nm laser light from the time-bin-state measurements. Intentionally blocking the transmission channel for brief periods during data collection allows us to synchronize these additional measurements with the QKD data.

Thermal and mechanical instabilities cause phase shifts between the TQE and MM-TQD, which we compensate with a motorized glass plate located in the long path of the TQE, manually optimizing for minimal QBER. An identical glass plate is placed in the long path of the MM-TQD to compensate glass-induced dispersion between the interferometers. Although channel delay fluctuations induced by atmospheric turbulence [22] are below our time-bin resolution, note also that the typical time scales of turbulence-induced phase shifts, on the order of 10 to 100 ms [23], significantly exceeds the temporal separation between our time-bins. Thus, the temporal delay each time-bin experiences during the passage of turbulence is effectively equal (as evidenced by the low QBER_time values measured).

3. Results

We first demonstrate the robustness of our system against atmospheric turbulence. To assess the quality of optical transmission through a turbulent channel, we characterize the channel's atmospheric coherence length, or Fried parameter [24], r_0. This parameter is inversely proportional to turbulence strength, and can quantify the cumulative turbulence effect over the entire free-space link. We estimate r_0 by analyzing the beam centroid motion through sequential CMOS sensor frames (see Fig. 2(a) and Appendix D). The measured atmospheric coherence lengths, averaged per second, fluctuate between 6 to 10 cm over the duration of our 600 s measurement, as shown in Fig. 2(b), with a mean value of r_0^{mean} = 7.83cm. For comparison, this is equivalent to a refractive-index-structure parameter C_n^2 of 2.78×10^{-15} m$^{-2/3}$. In a much less-turbulent channel with C_n^2 of 3.00×10^{-17} m$^{-2/3}$, Schmitt-Manderbach *et al* generated 28 bits/s of QKD key using a polarization encoding and a pulse rate of 10 MHz [25] (which would scale to 420 bits/s at 150 MHz repetition), while a C_n^2 of around 1.70×10^{-14} m$^{-2/3}$ is considered somewhat typical at sea-level, in the context of nighttime astronomical observations [26]. Despite the fluctuating coherence of the atmosphere, we observe relatively stable QBER$_{\text{time}}$ with a mean value of 5.32 %. Note that about 2 percentage points of QBER$_{\text{time}}$ stem from time-bin qubit source preparation, while synchronization blockages cause transient QBER spikes to around 50 %. We employ QKD post-processing of the data, including signal-to-noise filtering which suppresses contributions from these blockages, and generate secret keys at a rate of 154.2 bits/s in the asymptotic limit, under a total system loss of 38.4 dB (see Table 1 and Appendix B). In comparison, the visibility $V = 16$ % achievable at the decoder without lenses [6], with QBER $\geq (1 - V)/2$ [23], equates to a QBER of at least 42 %, well in excess of the 11 % bound for qubit-QKD protocols to succeed, even in principle.

Table 1. Measured QKD parameters, taken between 3 and 4 AM local time on August 17th, 2017. Low values of QBER$_{\text{time}}$ allow the creation of secret keys in the asymptotic regime.

	Turbulent	Turbulent & Depolarizing
Signal photons/ pulse	0.488	0.520
Decoy photons/ pulse	0.082	0.094
Background/ pulse	3.65×10^{-7}	3.45×10^{-7}
Channel loss (dB)	38.4	38.8
QBER$_{\text{time}}^{\text{mean}}$ (%)	5.32	5.08
Key rate (bits/s)	154.2	138.8

Next, we demonstrate our time-bin QKD system's robustness against depolarizing effects. To achieve these, we mix the polarization in the channel by continuously manipulating (by hand) the single-mode fiber that carries time-bin-encoded photons to the transmitter, i.e. rapid transforms of polarization. Then, for each density matrix ρ produced after 1 s of photon counting by the tomographic polarization analyzer at the receiver, we calculate the qubit purity of the measured polarization, $P = \text{Tr}(\rho^2)$. The effective achievable QBER for the polarization encoding, QBER$_{\text{pol}}$, is estimated via relating the purity P to QBER via the visibility $V = \sqrt{2P - 1}$ [27] (assuming rotationally symmetric noise). Such analysis then corresponds to finding the least QBER that could possibly be achieved by a polarization correction mechanism operating at a 1 Hz bandwidth.

Results are shown in Fig. 3. Projections of ρ along each of the Pauli bases (Fig. 3(b)) are spread over one large cluster, indicating significant variation of the polarization states. Over time the corresponding polarization state QBER values (Fig. 3(a)) fluctuate between almost pure (QBER$_{\text{pol}} \approx 0$ %) and almost completely mixed (QBER$_{\text{pol}} \approx 50$ %). Simultaneously, we observe steady time-bin QBER around the 5.08 % mean, with no correlation to polarization QBER. After
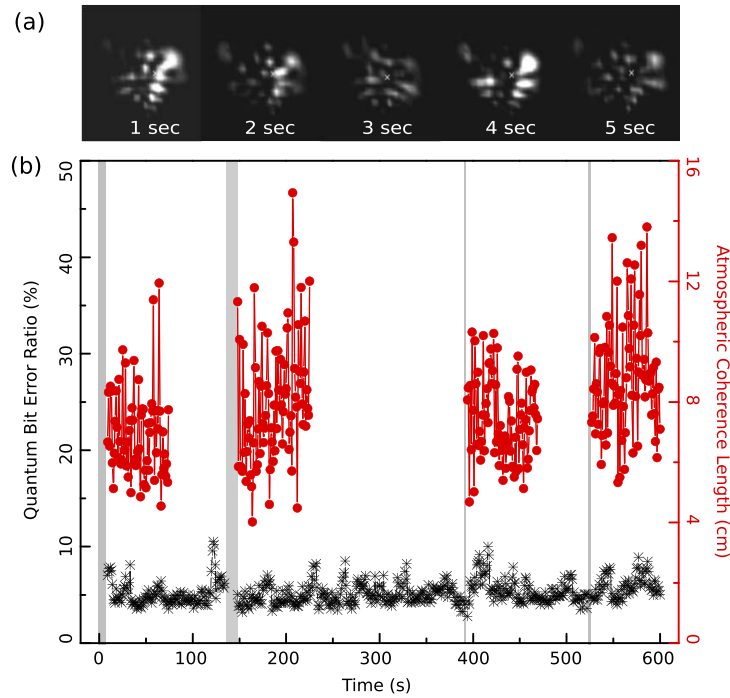
Fig. 2. **Characterization of the turbulent quantum channel of 1.2 km.** (a) Selected spatial-mode snapshots of incoming laser light at the receiver, captured by the CMOS sensor. A constant background pattern, caused by optical reflections, is significantly modulated by turbulence-induced distortion. (b) Despite short and fluctuating atmospheric coherence (red dots) of the optical link, low and steady values of $QBER_{time}$ (black asterisks) are observed. On occasion (highlighted by the grey areas), signals are intentionally blocked for synchronization.

post-processing of time-bin measurements, we find secure keys generated at a rate of 138.8 bits/s in the asymptotic regime, while polarization did not permit secure key generation.
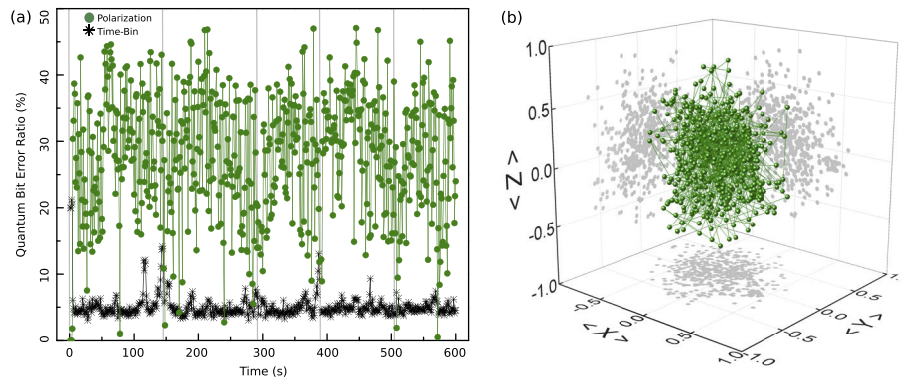

Fig. 3. **Characterization of the depolarizing and turbulent quantum channel.** (a) Green dots represent effective achievable $QBER_{pol}$ of polarization states through the channel, estimated from reconstructed density matrices. The measured stable $QBER_{time}$ (black asterisks) confirms robustness of the time-bin encoding against polarization mixture. Grey areas indicate when signals are blocked for synchronization. (b) Distribution of measured polarization expectation values.

4.   Conclusion

We experimentally demonstrated QKD using time-bin encoded photons in a free-space channel of 1.2 km range, under distortions of turbulence as well as turbulence & depolarization. Despite turbulence-induced wavefront distortions on the transmitted photons, our passive multi-mode time-bin qubit decoder remains efficient and of high interference-visibility, allowing the system to achieve a stable mean time-bin quantum bit error ratio of 5.32 %. This channel is capable of generating secure keys at a rate of 154.2 bits/s in the asymptotic limit. Moreover, in the presence of rapid polarization changes the error ratios remain essentially unchanged around 5.08%, with 138.8 bits/s asymptotic secure key rate. Our system could further be improved by miniaturzing the time-bin analyzer for better thermal stability, or by automating phase compensation. (Implementation of a reference-frame-independent protocol could even relax stability requirements of the time-bin interferometers.) Future study may also include development of a highly thermally stable unbalanced interferometer for analysis of time-bin states using different refractive index materials in each path, which could also allow extension into analysis of higher-dimensional states. By enabling quantum communication with time-bin encoding over multi-mode or depolarizing free-space channels, our demonstration opens possibilities to translate advanced fiber-based quantum protocols, such as coherent-one-way and differential-phase-shift quantum key distribution protocols, to long-distance free-space channels. Furthermore, encoding technologies used in quantum networks can be simplified by directly interfacing optical-fiber and free-space quantum links using time-bin-encoded photons.

Appendix A: Time-bin qubit encoder

We chose to utilize an available existing polarization-encoding source for convenience. (A direct time-bin encoding might reduce the overall complexity of the apparatus while increasing fidelity.) This source generates 785-nm-wavelength weak coherent pulses at 150 MHz that are polarization-encoded using a pair of electro-optical phase modulators in a balanced Mach-Zehnder interferometer [28]. Each pulse is initialized in one of four BB84 polarization states: horizontal ($|H\rangle$), vertical ($|V\rangle$), diagonal ($|D\rangle = (|H\rangle + |V\rangle)/\sqrt{2}$), or antidiagonal ($|A\rangle = (|H\rangle - |V\rangle)/\sqrt{2}$). The state is selected for each pulse following a randomized repeating sequence. (Though not secure, this does not invalidate the proof-of-principle conclusions we draw, and can be corrected with appropriate electronic engineering.) Signal and decoy intensity levels are controlled by a separate electro-optical intensity modulator, producing mean photon numbers per pulse of ≈ 0.5 and ≈ 0.1, respectively. These are measured at the transmitter with a calibrated pick-off and single-photon detector. Vacuum states are achieved by suppressing the laser trigger. Each intensity state appears in the sequence in proportions of 80 % (signal), 14 % (decoy), and 6 % (vacuum). After propagating through single-mode optical fiber, these pulses are then coherently converted to time-bin qubit states by an unbalanced polarizing Michelson interferometer [6], with path length difference matched to the MM-TQD. Polarization drifts in the fiber are corrected by a system that performs once-per-second tomographic reconstructions of a pick-off, and compensates using a quarter-, half-, quarter-wave plate triplet with optimized orientations [29].

Appendix B: Postprocessing for secret key generation

Due to restrictions of the available software, time correlation processing is performed at the transmitter—this is sufficient for our proof-of-principle demonstration, however a real-world implementation would have this analysis performed at the receiver or otherwise done in a way that suppresses the timing side-channel vulnerability [30]. Time correlation is done on per-second-aggregated data, with delays optimized on the number of source emission events coincident with reception events in the time-bin superposition basis. Early (optimized delay plus 2 ns) and late (optimized delay minus 2 ns) coincidences are then also identified. We

use a signal-to-noise filter to discard per-second regions with low count rate (under $500\,\mathrm{Hz}$), such as times when the signal is blocked to synchronize data across QKD, spatial-mode, and polarization measurements (these blockages are not included in the $600\,\mathrm{s}$ total measurement time). Such regions are treated as if no pulses were emitted from the source or detected by the receiver—otherwise, these sections would worsen the QBER due to the background noise [31]. The remaining data are basis-sifted to produce the sifted key. Error correction is accomplished using low-density parity-check codes: the receiver calculates an error correction syndrome from its sifted key based on a matrix constructed by the transmitter, which then uses this syndrome to reconcile its sifted key with the receiver's (observed error correction efficiency around 1.17). The resulting error-corrected keys are privacy amplified using an augmented Toeplitz matrix acting as a two-universal hash [32], producing the final secret key. We do not consider the effects of finite-size statistics, but calculate the length of the final key assuming the measured values extrapolate to the asymptotic limit.

Appendix C: Polarization preservation characterization

At the receiver, the 850-nm-wavelength light is analyzed in a tomographically complete basis set, consisting of horizontal/vertical, diagonal/antidiagonal, and right-circular/left-circular polarization projections by an arrangement of wave plates, beam splitters, and polarizing beam splitters (see Fig. 1). Photons are then coupled to multi-mode fibers and detected by Si-SPDs. For each 1 s integration of photon detection counts, maximum likelihood estimation [21] then reconstructs the density matrices of the polarization states. A completely pure state of polarization, within tomographic uncertainty, is measured when the single-mode fiber is untouched at the sender. Note that the polarization state undergoes a unitary rotation in the single-mode fiber that takes photons from the collection telescope to the tomographic analyzer. As the fiber is stationary, this unitary varies slowly over time (primarily due to temperature fluctuation), well outside the 1 s analysis time-scale. Because of this, the measured purity of the polarization state—and thus, the estimated achievable $\mathrm{QBER_{pol}}$—is accurate even though the actual rotation is not known.

Appendix D: Atmospheric coherence length

The atmospheric coherence length r_0 is directly related to the tilt angle variance of centroid displacement for two uncorrelated axes, $\sigma^2_{\text{2-axis}}$, as [33]

$$\sigma^2_{\text{2-axis}} = 0.364\left(\frac{D\lambda}{r_0^2}\right)^{5/3},\tag{1}$$

where $D = 12\,\mathrm{cm}$ is the initial beam diameter and $\lambda = 850\,\mathrm{nm}$ is its wavelength. We first subtract background noise from each CMOS sensor frame capture of the beam that may bias the center-of-mass calculation. The sensor frame rate for the data shown in Fig. 2(b) was $20\,\mathrm{Hz}$. Taking the centroid variance from the mean over 20 frames leads to a mean r_0 for each second of measurement.

Appendix E: Turbulence strength

The coherence lengths of an indoor atmosphere are measured for comparison to those of the outdoor free-space channel. For this we capture the spatial images of classical light at $850\,\mathrm{nm}$, co-propagated with time-bin quantum signal, using a CCD camera at a rate of $2\,\mathrm{Hz}$. From each captured frame a centroid value is calculated, and from the variations of these we calculate mean coherence lengths per second using Eq. (1). As shown in Fig. 4, the measured indoor values range from a few centimeters to several meters, yielding an average value of $l^{\text{avg}}_{\text{in}} = 65.8\,\mathrm{cm}$, which significantly exceeds the measured outdoor values of $l^{\text{avg}}_{\text{out}} = 7.83\,\mathrm{cm}$. In order to assess the degree

of r_0 fluctuation, we compute its standard deviation of $\sigma_{indoor} = 65.3\,\%$ and $\sigma_{outdoor} = 25.4\,\%$ (relative to their respective means) using data averaged over the same size of samples. We believe that the bigger variation in indoor measurement is caused by large and rapid temperature changes over a short part of the beam path, mainly owing to the building's heating and ventilation systems, which were co-located with the apparatus. The fact that the outdoor coherence length is much shorter than the indoor value despite slower temperature changes is because the heat fluctuation occurs over much longer distance.
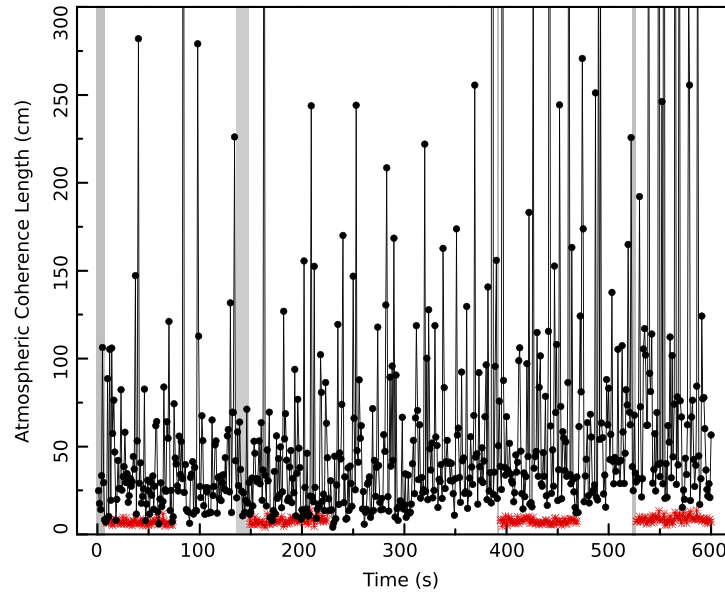

Fig. 4. Turbulence strength comparison. Measured coherence lengths of the outdoor channel (red asterisks) are much shorter than indoor values (black circles), showing that the spatial coherence of a photon will not be as well preserved over the longer outdoor transmission. The image recording rate for the outdoor (indoor) measurement is 20 Hz (2 Hz). Interruptions during the outdoor experiment are due to limited camera memory capacity. Upon resetting the camera, we intentionally blocked the beam (indicated by grey areas) to synchronize with single-photon detections.

Appendix F: Resolution of time bins in coincidence analysis

Figure 5 shows a typical time-correlation histogram for one second duration of measured detection events of transmission over the 1.2 km free-space channel. The histogram counts correspond to the number of detection events coincident with source emission events given a delta time offset. Early, late, and superposition time bins are clearly resolvable. The width of the time bins is dominated by the timing jitter of our single-photon detector, which is about 500 ps at the full width at half maximum. Clear separation between time bins, larger than timing jitter induced by any involved devices, is critical for communication.
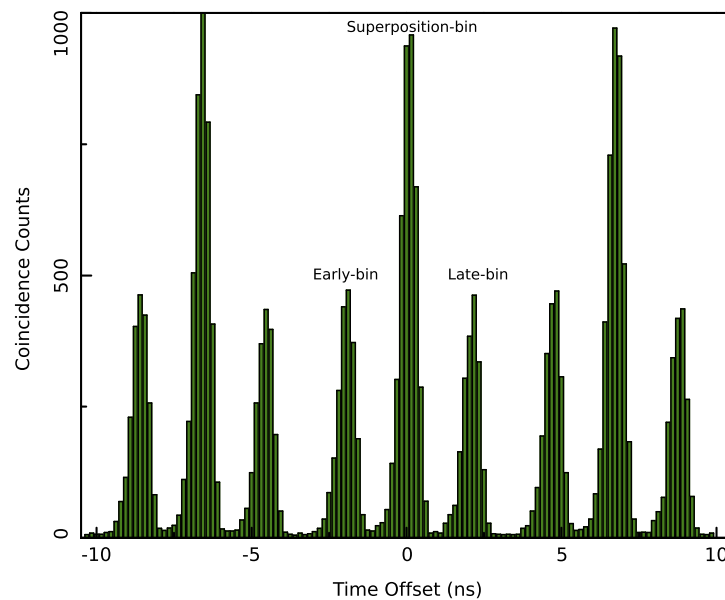
Fig. 5. Typical timing histogram. Shown are the counts of coincidences of source emissions with detection events, given a varying time offset between events at source and receiver (after correcting for delays, including the 4 μs free-space time-of-flight) and a 1 ns window, for one second of outdoor free-space link data. The time bins of the encoded quantum signal are clearly visible, with the central peak (around time offset 0) corresponding to the superposition basis, and the first minor peaks on either side corresponding to early and late states being measured. Other peaks originate from adjacent pulses, owing to the periodic pulsing of the weak-coherent pulse source, and are not coincidences of related events.

Funding

Disclosures

The authors declare no conflicts of interest.

References

1. H. J. Kimble, "The quantum internet," Nature **453**(7198), 1023–1030 (2008).
2. Y. He, X. Ding, Z.-E. Su, H.-L. Huang, J. Qin, C. Wang, S. Unsleber, C. Chen, H. Wang, Y.-M. He, X.-L. Wang, W.-J. Zhang, S.-J. Chen, C. Schneider, M. Kamp, L.-X. You, Z. Wang, S. Höfling, C.-Y. Lu, and J.-W. Pan, "Time-bin-encoded boson sampling with a single-photon device," Phys. Rev. Lett. **118**(19), 190501 (2017).
3. E. Saglamyurek, J. Jin, V. B. Verma, M. D. Shaw, F. Marsili, S. W. Nam, D. Oblak, and W. Tittel, "Quantum storage of entangled telecom-wavelength photons in an erbium-doped optical fibre," Nat. Photonics **9**(2), 83–87 (2015).
4. R. Valivarthi, M. G. Puigibert, Q. Zhou, G. H. Aguilar, V. B. Verma, F. Marsili, M. D. Shaw, S. W. Nam, D. Oblak, and W. Tittel, "Quantum teleportation across a metropolitan fibre network," Nat. Photonics **10**(10), 676–680 (2016).
5. N. T. Islam, C. C. W. Lim, C. Cahall, J. Kim, and D. J. Gauthier, "Provably secure and high-rate quantum key distribution with time-bin qudits," Sci. Adv. **3**(11), e1701491 (2017).
6. J. Jin, S. Agne, J.-P. Bourgoin, Y. Zhang, N. Lütkenhaus, and T. Jennewein, "Demonstration of analyzers for multimode photonic time-bin qubits," Phys. Rev. A **97**(4), 043847 (2018).
7. 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, L. Deng, T. Xi, L. Ma, T.

Hu, Q. Zhang, Y.-A. Chen, N.-L. Liu, X.-B. Wang, Z.-C. Zhu, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, "Satellite-to-ground quantum key distribution," Nature **549**(7670), 43–47 (2017).

8. A. Sit, F. Bouchard, R. Flickler, J. Gagnon-Bischoff, H. Larocque, K. Heshami, D. Elser, C. Peuntinger, K. Gunthner, B. Heim, C. Marquardt, G. Leuchs, R. W. Boyd, and E. Karimi, "High-dimensional intracity quantum cryptography with structured photons," Optica **4**(9), 1006 (2017).

9. M. Avesani, L. Calderaro, M. Schiavon, A. Stanco, C. Agnesi, A. Santamato, M. Zahidy, A. Scriminich, G. Foletto, G. Contestabile, M. Chiesa, D. Rotta, M. Artiglia, A. Montanaro, M. Romagnoli, V. Sorianello, F. Vedovato, G. Vallone, and P. Villoresi, "Full daylight quantum-key-distribution at 1550 nm enabled by integrated silicon photonics," arXiv: 1907.10039 (2019).

10. F. Steinlechner, S. Ecker, M. Fink, B. Liu, J. Bavaresco, M. Huber, T. Scheidl, and R. Ursin, "Distribution of high-dimensional entanglement via an intra-city free-space link," Nat. Commun. **8**(1), 15971 (2017).

11. H. Takenaka, M. Toyoshima, and Y. Takayama, "Experimental verification of fiber-coupling efficiency for satellite-to-ground atmospheric laser downlinks," Opt. Express **20**(14), 15301 (2012).

12. C. Liu, K. Pang, Z. Zhao, P. Liao, R. Zhang, H. Song, Y. Cao, J. Du, L. L. Li, H. Song, Y. Ren, G. Xie, Y.-F. Zhao, J. Zhao, S. M. H. Rafsanjani, A. N. Willner, J. H. Shapiro, R. W. Boyd, M. Tur, and A. E. Willner, "Single-end adaptive optics compensation for emulated turbulence in a bi-directional 10-mbit/s per channel free-space quantum communication link using orbital-angular-momentum encoding," Research **2019**, 1–10 (2019).

13. M. Chen, C. Liu, D. Rui, and H. Xian, "Performance verification of adaptive optics for satellite-to-ground coherent optical communications at large zenith angle," Opt. Express **26**(4), 4230 (2018).

14. G. Vallone, D. Dequal, M. Tomasin, F. Vedovato, M. Schiavon, V. Luceri, G. Bianco, and P. Villoresi, "Interference at the single photon level along satellite-ground channels," Phys. Rev. Lett. **116**(25), 253601 (2016).

15. I. N. Papadopoulos, S. Farahi, C. Moser, and D. Psaltis, "Focusing and scanning light through a multimode optical fiber using digital phase conjugation," Opt. Express **20**(10), 10583 (2012).

16. C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," Proc. IEEE Int. Conf. on Comput. Syst. Signal Process. **560**, 175–179 (2011).

17. W.-Y. Hwang, "Quantum key distribution with high loss: toward global secure communication," Phys. Rev. Lett. **91**(5), 057901 (2003).

18. X. B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography," Phys. Rev. Lett. **94**(23), 230503 (2005).

19. X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," Phys. Rev. A **72**(1), 012326 (2005).

20. J.-P. Bourgoin, E. Meyer-Scott, B. L. Higgins, B. Helou, C. Erven, H. Hübel, B. Kumar, D. Hudson, I. D'Souza, R. Girard, R. Laflamme, and T. Jennewein, "A comprehensive design and performance analysis of low earth orbit satellite quantum communication," New J. Phys. **15**(2), 023006 (2013).

21. J. B. Altepeter, E. R. Jeffrey, and P. G. Kwiat, "Photonic state tomography," Adv. At., Mol., Opt. Phys. **52**, 105–159 (2005).

22. L. Kral, I. Prochazka, and K. Hamal, "Optical signal path delay fluctuations caused by atmospheric turbulence," Opt. Lett. **30**(14), 1767 (2005).

23. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys. **74**(1), 145–195 (2002).

24. D. L. Fried, "Optical resolution through a randomly inhomogeneous medium for very long and very short exposures," J. Opt. Soc. Am. **56**(10), 1372 (1966).

25. T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter, "Experimental demonstration of free-space decoy-state quantum key distribution over 144 km," Phys. Rev. Lett. **98**(1), 010504 (2007).

26. D. H. Tofsted, S. G. O'Brien, and G. T. Vaucher, "An atmospheric turbulence profile model for use in army wargaming applications i," *Tech. Rep.* ARL-TR-3748 (2006).

27. F. Bussières, C. Clausen, A. Tiranov, B. Korzh, V. B. Verma, S. W. Nam, F. Marsili, A. Ferrier, P. Goldner, H. Hermann, C. Silberhorn, W. Sohler, M. Afzelius, and N. Gisin, "Quantum teleportation from a telecom-wavelength photon to a solid-state quantum memory," Nat. Photonics **8**(10), 775–778 (2014).

28. C. J. Pugh, S. Kaiser, J.-P. Bourgoin, J. Jin, N. Sultana, S. Agne, E. Anisimova, V. Makarov, E. Choi, B. L. Higgins, and T. Jennewein, "Airborne demonstration of a quantum key distribution receiver payload," Quantum Sci. Technol. **2**(2), 024009 (2017).

29. B. L. Higgins, J.-P. Bourgoin, and T. Jennewein, "Practical polarization-frame alignment for quantum key distribution with single-photon-level resources," arXiv:1810.04112 (2018).

30. A. Lamas-Linares and C. Kurtsiefer, "Breaking a quantum key distribution system through a timing side channel," Opt. Express **15**(15), 9388 (2007).

31. C. Erven, B. Heim, E. Meyer-Scott, J.-P. Bourgoin, R. Laflamme, G. Weihs, and T. Jennewein, "Studying free-space transmission statistics and improving free-space quantum key distribution in the turbulent atmosphere," New J. Phys. **14**(12), 123018 (2012).

32. J.-P. Bourgoin, N. Gigov, B. L. Higgins, Z. Yan, E. Meyer-Scott, A. K. Khandani, N. Lütkenhaus, and T. Jennewein, "Experimental quantum key distribution with simulated ground-to-satellite photon losses and processing limitations," Phys. Rev. A **92**(5), 052339 (2015).

33. R. K. Tyson, *Principle of Adaptive Optics* (CRC, 2010).