

Astronomical random numbers for quantum foundations experiments

Calvin Leung,^{1,*} Amy Brown,^{1,†} Hien Nguyen,^{2,‡} Andrew S. Friedman,^{3,§} David I. Kaiser,^{4,¶} and Jason Gallicchio^{1,**}

¹*Harvey Mudd College, Claremont, California 91711, USA*

²*NASA Jet Propulsion Laboratory, Pasadena, California 91109, USA*

³*University of California, San Diego, La Jolla, California 92093, USA*

⁴*Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA*

(Dated: July 18, 2017)

Photons from distant astronomical sources can be used as a classical source of randomness to improve fundamental tests of quantum nonlocality, wave-particle duality, and local realism through Bell’s inequality and delayed-choice quantum eraser tests inspired by Wheeler’s cosmic-scale Mach-Zehnder interferometer gedankenexperiment. Such sources of random numbers may also be useful for information-theoretic applications such as key distribution for quantum cryptography. Building on the design of an “astronomical random-number generator” developed for the recent “cosmic Bell” experiment [1], in this paper we report on the design and characterization of a device that, with 20-nanosecond latency, outputs a bit based on whether the wavelength of an incoming photon is greater than or less than 700 nm. Using the 1-meter telescope at the Jet Propulsion Laboratory (JPL) Table Mountain Observatory, we recorded the time of arrival of astronomical photons in both color channels from 50 stars of varying color and magnitude, 13 quasars with redshifts up to $z = 3.9$, and the Crab pulsar. For bright quasars, the resulting bitstreams exhibit sufficiently low amounts of mutual information and a sufficiently high ratio of astronomical detections to terrestrial noise to close both the locality and “freedom-of-choice” loopholes when used to set the measurement settings in a test of the Bell-CHSH inequality.

I. INTRODUCTION

Quantum mechanics remains extraordinarily successful empirically, even though many of its central notions depart strongly from those of classical physics. Clever experiments have been designed and conducted over the years to try to test directly such features as quantum nonlocality and wave-particle duality. Many of these tests depend upon a presumed separation between experimenters’ choices of specific measurements to perform and features of the physical systems to be measured. Tests of both Bell’s inequality and wave-particle duality can therefore make stronger claims about the nature of reality when the measurement bases are determined by events that are separated by significant distances in space and time from the rest of the experiment [1–5].

Bell’s inequality [6] sets a strict limit on how strongly correlated measurement outcomes on pairs of entangled particles can be, if the particles’ behavior is described by a local-realist theory. Quantum mechanics does not obey local realism and predicts that for particles in certain states, measurement outcomes can be correlated in excess of Bell’s inequality. (In a “local-realist” theory, no physical influence can travel faster than the speed of light in vacuum, and objects possess complete sets of

properties on their own, prior to measurement.) Bell’s inequality was derived subject to several assumptions, the violation of any of which could enable a local-realist theory to account for correlations that exceed the limit set by Bell’s inequality. (For recent discussion of such “loopholes,” see Refs. [7–9].) Beginning in 2015, several experimental tests have found clear violations of Bell’s inequality while simultaneously closing two of the three most significant loopholes, namely, “locality” and “fair sampling” [10–13]. To close the locality loophole, one must ensure that no information about the measurement setting or outcome at one detector can be communicated (at or below the speed of light) to the second detector before its own measurement has been completed. To close the fair-sampling loophole, one must measure a sufficiently large fraction of the entangled pairs that were produced by the source, to ensure that any correlations that exceed Bell’s inequality could not be accounted for due to measurements on some biased sub-ensemble.

Recent work has revived interest in a third major loophole, known as the “measurement-independence,” “settings-independence,” or “freedom-of-choice” loophole. According to this loophole, local-realist theories that allow for a small but nonzero correlation between the selection of measurement bases and some “hidden variable” that affects the measurement outcomes are able to mimic the predictions from quantum mechanics, and thereby violate Bell’s inequality [1, 2, 4, 5, 14–21].

A “cosmic Bell” experiment was recently conducted that addressed the “freedom-of-choice” loophole [1]. A statistically significant violation of Bell’s inequality was observed in measurements on pairs of polarization-entangled photons, while measurement bases for each de-

* cleung@g.hmc.edu

† afbrown@g.hmc.edu

‡ hien.t.nguyen@jpl.nasa.gov

§ asf@ucsd.edu

¶ dikaiser@mit.edu

** jason@hmc.edu

tector were set by real-time astronomical observations of light from Milky Way stars. (This experiment also closed the locality loophole, but not fair sampling.) The experiment reported in Ref. [1] is the first in a series of tests which aim to use the most cosmologically distant sources of randomness available, thus minimizing the plausibility of correlation between the setting choices and any hidden-variable influences that can affect measurement outcomes.

Random bits from cosmologically distant phenomena can also improve tests of wave-particle duality. Wheeler [22–24] proposed a “delayed-choice” experiment in which the paths of an interferometer bent around a distant quasar due to gravitational lensing. By making the choice of whether or not to insert the final beam splitter at the last instant, the photons end up behaving as if they had been particles or waves all along. (For a recent review, see Ref. [25].) Instead of using cosmic photons in the interferometer, a cosmologically distant source of randomness can be used to dictate run-by-run whether which-path information gets erased.

Likewise, an astronomical random-number generator could be used in delayed-choice quantum-eraser experiments. In a recent version of such a test [3], an (earth-bound) quantum random number generator was used to either erase or not erase which-path information and determine the particle- or wave-like nature of a photon going through an interferometer. By space-like separating this choice from the photon’s space-time path through the interferometer, interference fringes were erased or not based on a causally disconnected choice. In our new, proposed test, any local explanation of wave-particle duality would need to be expanded in scope to the time that the classical random bit was determined at the astronomical source, requiring correlations with our experiment from billions of years in the past.

Beyond such uses in tests of the foundations of quantum mechanics, low-latency astronomical sources of random numbers could be useful in information-theoretic applications as well. For example, such random bits could be instrumental for quantum-cryptographic key-distribution schemes (as also emphasized in Ref. [5]), further solidifying protocols like those described in Refs. [26–31].

In this paper, we describe the design choices and construction of an astronomical random-number generator, building on experience gained in conducting the recent “cosmic Bell” experiment [1]. In Section II we formalize and quantify what is required to close the freedom-of-choice loophole in tests of Bell’s inequality. This sets a minimum signal-to-noise ratio, which in turn dictates design criteria and choices of astronomical sources. In Section III we describe how astronomical random-number generators may be utilized in delayed-choice quantum-eraser experiments, to dramatically isolate the selection of measurements to be performed from the rest of the physical apparatus. In Section IV we compare different ways to turn streams of incoming astronomical photons

into an unpredictable binary sequence whose elements were determined at the time of emission at the astronomical source and have not been significantly altered since. After discussing the instrument design in Sections V–VII, we characterize in Section VIII the response of the instrument when observing a number of astronomical targets, including ≈ 50 bright Milky Way stars selected from the HIPPARCOS catalog having different magnitudes, colors, and altitudes. To verify the absolute and relative timing of our system, we observe the Crab pulsar, as described in Section IX. Finally, in Section X, we describe observations of 13 quasars with redshifts ranging from $z = 0.1 - 3.9$. In Section XI we discuss the ratio of quasar photons to “local” photons, quantify the predictability of the resulting bitstreams, and demonstrate the feasibility of using such quasars in the next round of “cosmic Bell” tests. Concluding remarks follow in Section XII.

II. CLOSING THE FREEDOM-OF-CHOICE LOOPHOLE IN BELL TESTS

To address the freedom-of-choice loophole in a cosmic Bell test, the choice of measurement basis on each side of the experiment must be determined by an event at a significant space-time distance from any local influence that could affect the measurement outcomes on the entangled particles [1, 4]. As we demonstrate in this section, an average of at least $\approx 79\%$ of detector settings on each side must be generated by information that is astronomical in origin, with a higher fraction required in the case of imperfect entanglement visibility. We will label detector settings that are determined by genuinely astronomical events as “valid,” and all other detector settings as “invalid.” Thus, we will use this framework to analyze random numbers obtained from both stars and quasars. As we will see in later sections, “invalid” setting choices can arise for various reasons, including triggering on local photons (skyglow, light pollution) rather than astronomical photons, detector dark counts, as well as by astronomical photons that produce the “wrong” setting due to imperfect optics.

Experimental tests of Bell’s inequality typically involve correlations between measurement outcomes $A, B \in \{-1, +1\}$ for particular measurement settings (a_k, b_ℓ) , with $k, \ell \in \{1, 2\}$. Here a and A refer to the measurement setting and outcome at Alice’s detector (respectively), and b and B refer to Bob’s detector. We follow the notation of Ref. [1] and write the Clauser-Horne-Shimony-Holt (CHSH) parameter, S [32], in the form

$$S \equiv |E_{11} + E_{12} + E_{21} - E_{22}|, \quad (1)$$

where $E_{k\ell} = 2p(A = B|a_k b_\ell) - 1$, and $p(A = B|a_k b_\ell)$ is the probability that Alice and Bob measure the same outcome given the joint settings (a_k, b_ℓ) . Bell’s inequality places a restriction on all local-realist theories. In terms

of the quantity S , the Bell-CHSH inequality takes the form $S \leq 2$ [32].

The value of S that one measures experimentally may be expressed as a linear combination of S_{valid} , due to astronomical setting choices, and S_{invalid} , due to non-astronomical setting choices. We may write

$$S_{\text{exp}} = qS_{\text{valid}} + (1 - q)S_{\text{invalid}}, \quad (2)$$

where q is the probability that both setting choices are generated by a given pair of astronomical sources for a given experimental run. We conservatively assume that a local-realist theory could exploit the freedom-of-choice loophole to maximize S_{exp} by engineering each invalid experimental run to yield the mathematical maximum of $S_{\text{invalid}} = 4$, while we assume that each valid run would be limited to $S_{\text{valid}} \leq 2$ by the usual Bell-CHSH argument. A “relaxed” version of the Bell-CHSH inequality is then $S_{\text{exp}} \leq 4 - 2q$. This makes the statistical significance of any experimental Bell violation highly sensitive to the fraction of valid settings generated. Since quantum mechanics predicts a maximum value $S_{\text{QM}} = 2\sqrt{2}$ [33], and since $S_{\text{exp}} \leq 4 - 2q \leq S_{\text{QM}}$, we conclude that for a cosmic Bell experiment to distinguish between the predictions of quantum mechanics and a local-realist alternative that exploits the freedom-of-choice loophole, we must be able to conduct a sufficiently high fraction q of our experimental runs using valid astronomical photons:

$$q \geq 2 - \sqrt{2}. \quad (3)$$

In this framework, there are local-realist models in which only one detector’s setting choice needs to be influenced or predicted by a hidden-variable mechanism in order to invalidate a given experimental run and produce $S = 4$. We conservatively assume that corrupt settings do not occur simultaneously, allowing the local-realist alternative to maximally exploit each one. Hence, the overall fraction of valid settings must be at least $q = 1 - p^{\text{Alice}} - p^{\text{Bob}}$, where $p^{(i)}$ is the probability that a setting at the i^{th} detector is invalid, with $i = (\text{Alice}, \text{Bob})$. Defining $q^{(i)} = 1 - p^{(i)}$ as the fraction of valid settings on a particular side, the requirement in Eq. (3) may be written

$$q^{\text{Alice}} + q^{\text{Bob}} \geq 3 - \sqrt{2}. \quad (4)$$

For simplicity, if we assume that the experiment is symmetric with $q^{\text{Alice}} = q^{\text{Bob}} = q^*$, we find that $q^* \geq (3 - \sqrt{2})/2 \simeq 79.3\%$. Thus, for a symmetric setup, roughly eight out of ten photons incident on each random number generator need to be of astronomical origin. When choosing a scheme for generating random numbers, it is necessary to keep this “signal-to-noise” threshold in mind.

It is also important to consider that it is very difficult in practice to achieve a value of S close to the quantum-mechanical maximum of $2\sqrt{2} \approx 2.83$, due to imperfections in the experimental setup. For example,

the first cosmic Bell test obtained values of $S_{\text{exp}} = 2.43$ and $S_{\text{exp}} = 2.50$ [1]. Under such conditions, q would need to be correspondingly higher to address the freedom-of-choice loophole. Also, the closer the measurement of S_{exp} is to the validity-modified local-realist bound, the more experimental runs are required to achieve a statistically significant Bell violation. Hence the “eight-out-of-ten” rule derived here represents the bare minimum to close the freedom-of-choice loophole for pure entangled states and robust statistics with many experimental runs. In later sections we measure different sources of invalid detections and find quasars that are on both sides of this usefulness bound with our telescope.

III. DELAYED-CHOICE EXPERIMENTS

Another application of an astronomical random-number generator is to use it in an experiment to test wave-particle duality. The concept of testing wave-particle duality with a Mach-Zehnder interferometer was first proposed by John Archibald Wheeler [22–24] and has been realized via a laboratory-scale Mach-Zehnder interferometer [34]. Wheeler proposed using the light from a doubly gravitationally-lensed source of astronomical photons as a Mach-Zehnder interferometer of cosmological scale, coupling each image into two inputs of a beamsplitter. Observation of interference at the output would suggest that the light took both paths around the gravitational lens and interfered at the beamsplitter, acting as a wave. Removing the beamsplitter in the Mach-Zehnder interferometer would prevent the light from recombining, and the astronomical light would manifest itself as single photons which appear at one output or the other but not both. If one rejects wave-particle duality, the logical conclusion is that either the choice of inserting the beamsplitter in the final moments of the light’s journey somehow retrocausally affected the light’s trajectory across the cosmos, or that the choice of inserting the beamsplitter was predictable by the light before it embarked on its journey. (See also Ref. [25].)

Rather than try to interfere astronomical photons with a gravitational lens, we can realize a similar experiment that leads to the same logical conclusion. Instead of testing the wave-particle duality of an astronomical photon, we may use a standard tabletop Mach-Zehnder interferometer, and use astronomical setting choices to determine whether to insert or remove the beamsplitter. In such a setup, the choice of which measurement to perform would be made in a causally disconnected way from the particulars of the behavior of the photon in the interferometer, billions of years before the interferometer photon had even been created. In this experiment as well as Wheeler’s original gedankenexperiment, separating the choice of inserting the beamsplitter from both the creation of the photon and its journey makes alternate explanations of wave-particle duality implausible.

Nevertheless, there would still exist a local-realist ex-

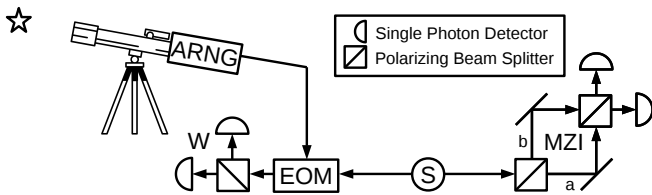


FIG. 1. A proposed experiment to test wave-particle complementarity, in the spirit of Wheeler’s “delayed-choice” experiment. In our version of a delayed-choice experiment, two-photon entangled states are produced at S , sending one entangled partner (the “environment” photon) towards W and the other (the “signal” photon) toward a Mach-Zehnder interferometer (MZI). An astronomical random-number generator (ARNG) activates an electro-optical modulator (EOM) in order to rapidly set the measurement basis for the environment photon at W , potentially revealing which-path information about the signal photon. The signal photon at the MZI acts as a particle or a wave accordingly, even though the choice of whether to reveal which-path information is made in a causally disconnected way, potentially billions of years before the experiment has been run.

planation for the outcomes of such an experiment. Two local-hidden-variable-like surrogates of the photon that travels around the interferometer could each take one of the two paths and accumulate a phase based on their distance traveled. When they come together, they will either see a beam splitter or not. They can either combine their accumulated phases and act like a wave or they can ignore their phases and pick one detector over the other in some deterministic or locally-probabilistic way. In this way, there would exist a perfectly local-realist explanation for the wave-particle duality manifested by single particles.

On the other hand, the outcomes of two-photon experiments such as a delayed-choice quantum eraser cannot be accounted for within a local-realist framework. In modern delayed-choice quantum-eraser experiments [3], wave-particle duality is tested by interfering one entangled partner (the “signal” photon) of a two-photon entangled state in a Mach-Zehnder interferometer. Rather than removing the beamsplitter in the Mach-Zehnder interferometer, a measurement of the other entangled partner (the “environment” photon) is made outside the light cone of the signal photon to erase which-path information. This can be done at the same time or after the signal photon propagates through the interferometer [3, 25]. See Fig. 1.

In the language of quantum mechanics, these experiments begin with a polarization-entangled state of “signal” and “environment” photons. Following the discussion in Ref. [3], we may write such a state as

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|H\rangle_s|V\rangle_e + |V\rangle_s|H\rangle_e). \quad (5)$$

When the signal photon enters the polarizing beamsplitter at the start of the interferometer, its polarization

state gets mapped onto its path (a or b) through the interferometer. The state then becomes

$$|\psi\rangle \rightarrow \frac{1}{\sqrt{2}}(|b\rangle_s|V\rangle_e + |a\rangle_s|H\rangle_e). \quad (6)$$

If the environment photon is measured in the horizontal/vertical basis, either result collapses the state, revealing which-path information, and no interference is observed at the second polarizing beamsplitter. If, however, the environment photon is measured in the circular basis, the signal photon enters into a superposition of both paths. In that case, the state can be written as

$$|\psi\rangle \rightarrow \frac{1}{2} [(|a\rangle_s + i|b\rangle_s)|L\rangle_e + (|a\rangle_s - i|b\rangle_s)|R\rangle_e]. \quad (7)$$

After the final beamsplitter, the paths will combine and interfere. In each term, the amplitude for each detector to fire becomes a function of the relative phase due to path-length differences around the interferometer. Conditioned on whether the environment photon is left- or right-circularly polarized, the signal photon’s interference fringes will be 180 degrees out of phase.

For both linear and circular basis choices, the signal photon enters each detector with equal probability, so as with any entangled state, information cannot be sent simply by choosing a measurement basis. Interference fringes or the lack thereof can only be seen when one sorts the signal photon’s detections into categories based on the basis choice and measurement result of the environment photon. As in tests of Bell’s inequality, any apparent nonlocality is only nonlocality of correlations.

Any local explanation of the nonlocal correlations in this experiment would rely on being able to predict whether the measurement of the environment photon erases or reveals which-path information of the signal photon, dictating the wave-like or particle-like behavior of the signal photon. Setting the environment photon’s measurement basis with a single astronomical random-number generator can be used to dramatically constrain the potential origins of this predictability.

IV. GENERATING ASTRONOMICAL RANDOMNESS

We consider the two potential schemes for extracting bits of information from astronomical photons to use as sources of randomness for use in experiments like those described in Sections II-III. In general, it is important that the information extracted be set at the time of the astronomical photon’s emission, rather than at the time of detection or any intervening time during the photon’s propagation. We deem the setting corrupt if this condition is not met, and we evaluate two methods with particular emphasis on the mechanisms by which corruption may occur.

A. Time of Arrival

The first method is to use the time-of-arrival of the astronomical photons, rather than their color, to generate bits [4, 5]. We can choose to map time tags to bits based on whether some pre-specified decimal place of the timestamp is even or odd. For example, a 0 could correspond to the case of a photon arriving on an even nanosecond, and a 1 for arrival on an odd nanosecond. The main advantage of this scheme is its simplicity: since timestamps need to be recorded to close the locality loophole, there is no need for additional hardware to generate random settings. In addition, it will always be possible to ensure a near-50/50 split between the two possible setting choices at each side of the experiment regardless of the nature of the astronomical source of randomness.

The primary disadvantage of this scheme is that it is very difficult to quantify galactic and terrestrial influences on the recorded timestamp of the photon’s arrival. It is necessary that we be able to quantify the fraction of photons that are corrupt, as discussed in Section II. In the remainder of this section, we consider the constraints on which decimal place in the detection timestamp should be used to generate random bits.

It is tempting to condition setting choices on the even/oddness of a sub-nanosecond decimal place, making use of deterministic chaos and apparent randomness. However, the timestamp of a given photon’s arrival at this level of precision is susceptible to corruption from myriad local influences which are difficult (perhaps impossible) to quantify, such as effects in the interstellar medium, turbulence in the atmosphere, and timing jitter in the detectors or time-tagging unit, which may affect the even-odd classification of nanosecond timestamps. The atmosphere has an index of refraction $n \approx 1 + 2.9 \times 10^{-4}$, which in a 10 km-thick atmosphere corresponds to the photons arriving ~ 10 ns later than they would if traveling in a vacuum [35]. Thus, relying upon any decimal place less significant than the tens-of-nanoseconds place to generate a bit admits the possibility of the atmosphere introducing some subtle delay and corrupting the generated bits.

Choosing a setting by looking at the even or odd microsecond timestamps, on the other hand, makes it difficult to close the locality loophole in tests of Bell’s inequality. For example, the first cosmic Bell test used a setup whose baseline length constrained the maximum timescale of a single run to $< 3 \times 10^{-6}$ s [1], based on the distance between the source of entangled particles and the closer of the two measurement stations. It is difficult to choose a timescale that is long enough to be insensitive to subtle, unquantifiable influences, yet short enough to satisfy the locality conditions of the experiment.

In addition, using even/odd timestamps to determine the setting choice admits the possibility that a local hidden variable theory synchronizes its “entangled” photon emissions to coincide with a particular setting choice. For these reasons, using the timestamp of astronomi-

cal photons’ arrivals does not appear to be an optimal method for generating unpredictable numbers of astronomical origin.

B. Colors

An alternate approach, developed for use in the recent cosmic Bell test [1], is to classify astronomical photons by designating a central wavelength λ' and mapping all detections with $\lambda < \lambda'$ to 0 and detections with $\lambda > \lambda'$ to 1 using dichroic beamsplitters with appropriately chosen spectral responses. The advantage of the wavelength scheme is that possible terrestrial influences on photons as a function of wavelength are well-studied and characterized by empirical studies of astronomical spectra, as well as studies of absorption and scattering in the atmosphere. In contrast to effects which alter arrival times, the effects of the atmosphere on the distribution of photon wavelengths varies over the course of minutes or hours, as astronomical sources get exposed to a slowly-varying airmass over the course of a night-long Bell test. The airmass, and therefore the atmosphere’s corrupting influence on incoming astronomical photons, can be readily quantified as a function of time.

One important advantage of using astronomical photons’ color stems from the fact that in an optically linear medium, there does not exist any known physical process that could absorb and re-radiate a given photon at a different wavelength *along our line of sight*, without violating the local conservation of energy and momentum [1]. For photons of genuinely cosmic origin, certain well-understood physical processes do alter the wavelength of a given photon between emission and detection, such as cosmological redshift due to Hubble expansion, and gravitational lensing. Neither of these effects, however, should be an impediment to using astronomical photons’ color to test local-realist alternatives to quantum mechanics.

The effects of cosmological redshift are independent of a photon’s wavelength at emission, and hence treat all photons from a given astronomical source in a comparable way [36, 37]. Gravitational lensing effects are also independent of a photon’s wavelength at emission [38], though lensing accompanied by strong plasma effects can yield wavelength-dependent shifts [39]. Even in the latter case, however, any hidden-variable mechanism that might aim to exploit gravitational lensing to adjust the detected wavelengths of astronomical photons on a photon-by-photon basis would presumably need to be able to manipulate enormous objects (such as neutron stars) or their associated magnetic fields (with field strengths $B > 10^8$ Gauss) with nanosecond accuracy, which would require the injection or removal of genuinely astronomical amounts of energy. Thus, whereas some of the original hidden-variable models were designed to account for (and hence be able to affect) particles’ trajectories [40, 41] — including, thereby, their arrival times at

a detector — any hidden-variable mechanism that might aim to change the color of astronomical photons on a photon-by-photon basis would require significant changes to the local energy and momentum of the system.

The chief disadvantage of using photons’ color in an astronomical random-number generator is that the fluxes of “red” ($\lambda > \lambda'$) and “blue” ($\lambda < \lambda'$) photons will almost never be in equal proportion, and hence will yield an overall red-blue statistical bias. Such bias in itself need not be a problem: one may conduct Bell tests with bias in the frequency with which various detector-setting combinations are selected, by taking account of such bias (or “excess predictability”) in the analysis of the statistical significance of any measured violation of Bell’s inequality [1, 9]. However, a large red-blue bias does affect the duration of an experiment — whose duration is intrinsically limited by the length of the night — because collecting robust statistics for each of the four joint setting choices (a_k, b_ℓ) would prolong the experiment.

A second disadvantage comes from imperfect alignment. If the detectors for different colors are sensitive to different locations on the sky, atmospheric turbulence can affect the paths of photons and the relative detection rates. We see evidence of this effect at the sub-percent-level in the measurements described in Sections VIII-X: the next photon has a slightly increased probability of being detected as the same color as the previous few photons. We quantify this effect in terms of mutual information in Section XI.

We devote the remainder of this paper to the photon-color scheme, given its advantages over the timestamp scheme. Any time-tagging hardware that outputs bits based on color can also output bits based on timing. Our time tags pass every test of randomness in the NIST Statistical Test Suite for which we had sufficient bits to run them [42]. One may also use the logical XOR of color and timing bits.

V. DESIGN CONSIDERATIONS

As became clear during the preparation and conduct of the recent cosmic Bell experiment [1], in designing an instrument that uses photon colors to generate randomness, it is necessary to begin with a model of how settings become corrupted by local influences, and make design choices to minimize this. In this section we build on the discussion in Ref. [1] to characterize valid and invalid settings choices.

One obvious source of potential terrestrial corruption is from background noise, due to thermal fluctuations in the detector (or “dark counts”), as well as background light from the atmosphere (or “skyglow”). We designate the sum of these two rates as $n_j^{(i)}$, where j labels the two detector arms (red and blue) and i labels the two random number generators (Alice and Bob) in a test of Bell’s inequalities. If we measure a count rate of $r_j^{(i)}$ when

pointing at an astronomical source, then the probability of obtaining a noise count is simply $n_j^{(i)}/r_j^{(i)}$. In selecting optics, it is important to select single-photon detectors which have low dark count rates and a small field of view on the sky in order to minimize this probability.

A second source of terrestrial corruption is misclassification of photon colors. A typical way to sort photons by color is to use a dichroic beamsplitter. However, due to imperfections in the dichroic beamsplitter’s spectrum, there is a nonzero probability that a photon in the “red” wavelength range is transmitted towards the arm designated for “blue” photons and vice versa. We need to select dichroic beamsplitters with high extinction ratios and steep transitions such that the probability of misclassification is minimal.

To quantify the contribution from imperfect dichroic mirrors, we define j' to be the color opposite to j , that is, red if j refers to blue and vice versa. Depending on the source spectrum, some fraction $f_{j' \rightarrow j}^{(i)}$ of photons end up in the j^{th} arm, despite being of the j'^{th} color. If $s_j^{(i)}$ astronomical photons per second of color j are intended for the i^{th} detector, photons leak into the j^{th} arm at a rate of $f_{j \rightarrow j'} s_j^{(i)}$. Knowing $r_j^{(i)}$, $n_j^{(i)}$, as well as the mixture rates $f_{j' \rightarrow j}$, $f_{j \rightarrow j'}$ allows us to “unmix” the observed count rates r_j to back out the true fluxes $s_j^{(i)}$.

In summary, the rate that the j^{th} detector arm in the i^{th} detector yields a corrupt setting is at most the sum of the noise rate, $n_j^{(i)}$, and the rate of misclassifications from the j'^{th} arm, $f_{j' \rightarrow j} s_{j'}^{(i)}$. Since the total observed count rate is $r_j^{(i)}$, the probability of obtaining an incorrect setting is

$$p_j^{(i)} = \frac{n_j^{(i)}}{r_j^{(i)}} + \frac{s_{j'}^{(i)} f_{j' \rightarrow j}}{r_j^{(i)}}. \quad (8)$$

The overall probability of corruption for a bit is conservatively estimated by maximizing over its red and blue detector arms. Since the overall probability of corruption is not necessarily the same for Alice and Bob, we denote this invalid-bit probability $p^{(i)}$, where

$$p^{(i)} = \max(p_{\text{red}}^{(i)}, p_{\text{blue}}^{(i)}) = 1 - q^{(i)}, \quad (9)$$

where the average of the two valid-bit probabilities $q^{(i)}$ needs to be at least 79.3%, as discussed in Section II. Note that the j index labels individual detector arms, whereas the i index labels different observer’s detectors after maximizing over each detector’s arms.

To minimize an individual detector arm’s corruption probability p_j , it suffices to minimize the quantities n_j by minimizing the dark count and skyglow rates, and to choose high-quality dichroic beamsplitters to minimize $f_{j' \rightarrow j}$. The total count rate, r_j , is maximized when the atmosphere is most transparent: thus, we will designate our red and blue observing bands to roughly coincide with the near-infrared (700 nm – 1150 nm) and optical (350 nm – 700 nm) respectively [1, 4].

Several other design considerations are equally important. The instrument must be able to point to dim and distant target objects, which are typically high-redshift quasars. The dimness of even the brightest high-redshift quasars in optical and near-infrared (NIR) wavelengths not only makes it difficult to establish the high signal-to-noise ratio required, but also makes tracking objects non-trivial over the duration of a Bell test, which can last for hours. At the same time, the instrument must generate settings at a sufficiently high rate to perform the experiment. Each run of a Bell inequality test only closes the locality and freedom-of-choice loopholes if valid settings from quasars arrive on both sides within a time window whose duration is set by the light-travel time between Alice and Bob. Thus having a high collection efficiency of the quasar light is doubly important.

VI. INSTRUMENT

Our astronomical random-number generator incorporates several design features that were developed in the course of preparing for and conducting the recent cosmic Bell experiment [1]. A schematic of our new instrument, constructed at the Harvey Mudd College Department of Physics, is shown in Fig. 2 and a photo in Fig. 3. It is housed in a box made of black Delrin plastic of dimensions $30 \times 30 \times 10$ centimeters and weighs 5.5 kg, most of which is the weight of two single-photon detectors and the astronomical pointing camera. The instrument was mounted at the focus of a 1-meter aperture, 15-meter focal-length telescope at the NASA Jet Propulsion Laboratory’s Table Mountain Observatory. The light from the telescope is coupled directly into our instrument’s aperture without using optical fibers to reduce coupling losses.

The telescope is focused onto a $200 \mu\text{m}$ pinhole on a Lenox Laser 45° pinhole mirror. The size of this pinhole was chosen to minimize skyglow background (and therefore the predictability due to skyglow) by matching the 2-3 arcsecond astronomical seeing at the Table Mountain site. This pinhole size corresponds to 2.75 arcseconds on our 15 m focal-length telescope. The incoming light that does not make it through the pinhole is reflected by the mirror and reimaged through a Canon EF-S 60mm F2.8 macro lens onto a ZWO ASI 1600MM cooled $4/3$ ” CMOS camera, which aids in finding and positioning the source into the pinhole. Real-time monitoring of this camera was used to guide the telescope in some observations and to capture long exposures as in Fig. 4 and Fig. 5.

The light from the object of interest that makes it through the pinhole gets collimated by a 25 mm diameter, 50 mm focal-length lens. This collimated light gets split by a 697 nm short-pass dichroic beamsplitter (Semrock F697-SDi01-25x36). The mostly-visible light (denoted “blue”) passes through and gets imaged onto one IDQ ID120 Silicon Avalanche Photodiode detector through a 25 mm diameter, 35 mm focal-length lens. The image

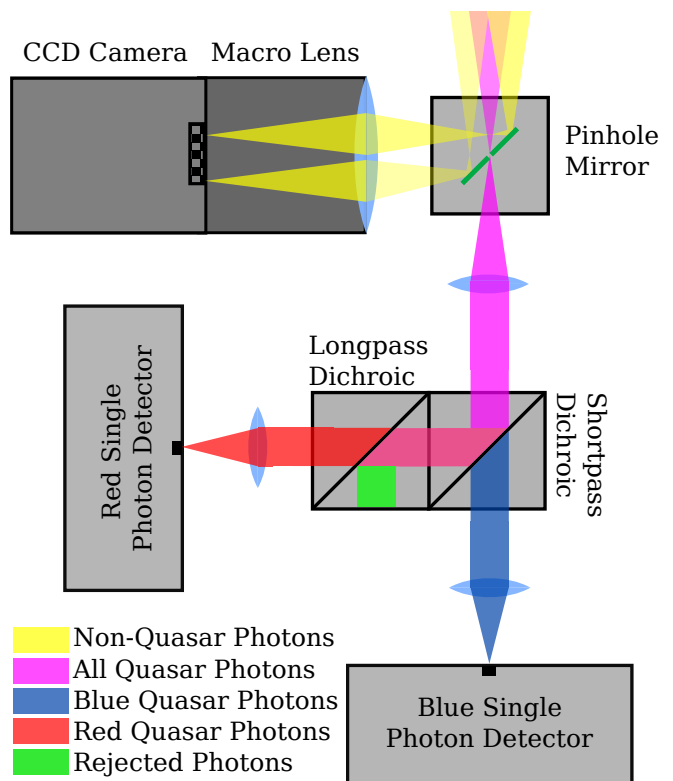


FIG. 2. This figure shows the intended optical paths of our astronomical random-number generator (not to scale). Astronomical light from multiple objects in the field of view of the telescope enters at the top right of the schematic. This light is brought to a focus by the telescope onto the plane of the pinhole mirror. Most of the light is reflected by the mirror (yellow) and refocused onto a CCD. However, light from an object of interest (purple) passes through the pinhole, and is then collimated and sorted by color via a system of one shortpass and one longpass dichroic beamsplitter. These beams (red and blue) are refocused onto the active area of our two avalanche photodiodes for detection and timestamping. The placement of the dichroics is similar to the fiber-coupled scheme used in Ref. [1].

of the pinhole is reduced to $140 \mu\text{m}$ in diameter, which is well within the ID120’s $500 \mu\text{m}$ active area, making for reliable alignment and minimal concern about aberrations and diffraction. This alignment was performed by mounting the final lens on an XY stage attached to the detector—collimated light hitting the lens slightly off axis will form an image slightly off axis.

The mostly-infrared (IR) light reflects off of the first dichroic onto a 705 nm long-pass dichroic beamsplitter (Semrock FF705-Di01-25x36). Here the small amount of reflected light (mixed visible/IR) is ignored, but the IR light that passes through the second dichroic is imaged by an identical 35 mm focal-length lens onto an identical ID120 detector. In preparing for the recent cosmic Bell experiment [1], it was determined that two dichroics were necessary because a single dichroic’s optical density was low enough such that a non-negligible fraction of the



FIG. 3. Photo of our astronomical random-number generator in the laboratory with the lid off and dichroic mirrors exposed.

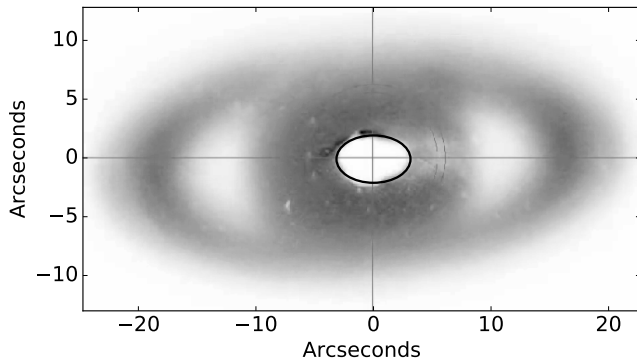


FIG. 4. Using the date of observation (3 July 2016) and the coordinates of Table Mountain Observatory, it is possible to compute the angular diameter of Saturn. This enables us to estimate the size of the pinhole as an ellipse with semimajor axes of 2.01 and 3.15 arcseconds. The horizontal and vertical lines running through the pinhole are crosshairs to guide the eye. The field of view calculated via Saturn is consistent with the field of view computed using telescope and camera parameters.

light could go either way and would not be determined by the astronomical object. This arrangement of having the detector after a transmission rather than a reflection was chosen because the light transmitted through these dichroics has less contamination than the reflected light. The particular pair was selected to minimize the wrong-way fraction $f_{j \rightarrow j'}$ from Section V, while maximizing the overall detections and roughly splitting the detector's spectral response in half.

To detect astronomical photons, we chose ID120 Sili-

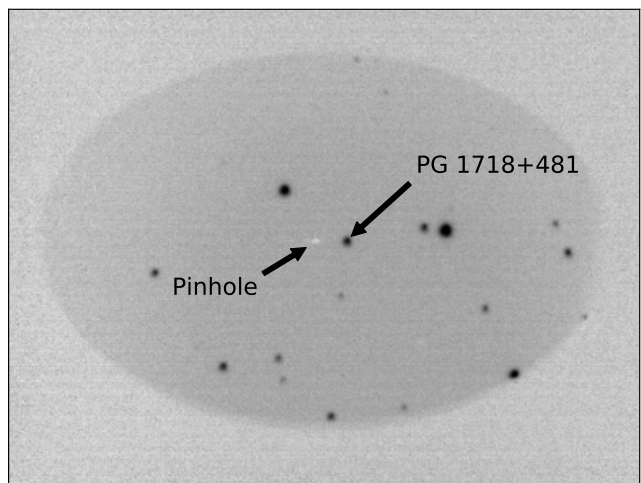


FIG. 5. Dim objects such as the quasar PG 1718 + 481 (shown here) were identified by comparing the local field to astronomical catalogs. Dark counts were typically recorded by keeping the object a few spot-sizes away from the pinhole, for example, as the telescope is positioned here.

con Avalanche Photodiode Detectors (APDs) that have up to 80% quantum efficiency between 350 and 1000 nm, a $500 \mu\text{m}$ active area so the image of the pinhole fits well within the active area, and a low ($< 100 \text{ Hz}$) specified dark count rate. These have 300 ps of timing jitter with an artificially extended deadtime of 420 ns to prevent afterpulsing. They have a photon-to-electrical-pulse latency of up to 20 ns. The detectors' active area was cooled to -40°C and achieved a measured dark count rate of 40 Hz. At zenith, the background rates due to skyglow are roughly 20 Hz and 60 Hz in the blue and red arms respectively. (For comparison, the quasars we observed had rates of 100 to 1000 Hz in each channel.) The reason for this asymmetry results from a combination of different optical coupling efficiencies in each arm and the spectrum of the background skyglow, which tends to be brighter in the near-infrared than in the visible band.

Signals from the APDs are recorded by an IDQ ID801 Time to Digital Converter (TDC). The relative precision of time-tags is limited by the 80.955 ps clock rate of the TDC, and by the 300 ps timing jitter on the APD. Count rates as a function of time for dark counts and several stars and quasars are shown in Fig. 6.

As a timing reference, we also record a stabilized 1-pulse-per-second signal from a Spectrum Instruments TM-4 GPS unit. (Absolute time can also be recorded using this GPS unit's IRIG-B output.) The GPS timing solution from the satellites is compensated for the length of its transponder cable, which corresponds to a delay of 77 ns.

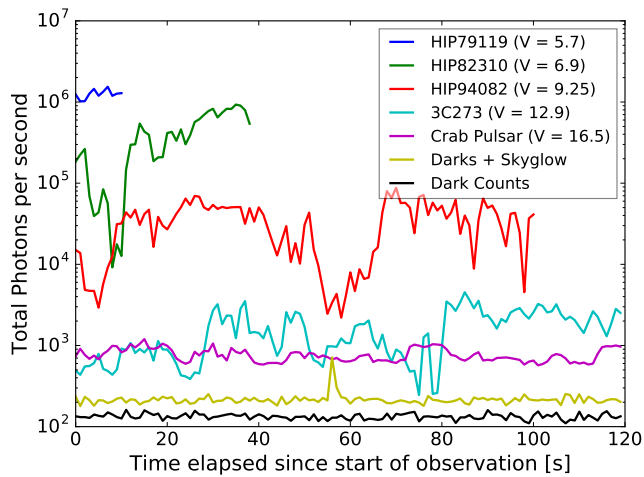


FIG. 6. The total count rate over time for various sources fluctuates dramatically due to 2 – 3 arcseconds of seeing and telescope pointing, which are on the order of our pinhole size. The legend entries appear in the same vertical ordering as on the plot. The small spike in the “Darks + Skyglow” trace is likely from a small object such as a plane or satellite that briefly passed through our field of view, or headlights from a car. The Crab Pulsar’s count rate is unusually stable over time because the nebula has an extent of several arcminutes.

VII. SPECTRA: ATMOSPHERE, LENSES, DICHOIRCS, DETECTOR RESPONSE

Building on the analysis in Ref. [1], we formulate a model of the instrument’s spectral response in each arm to characterize its ability to distinguish red from blue photons. The aim of this section is to compute for our instrument the $f_{j \rightarrow j'}$ parameters, defined as the probability that photons of type j are detected as photons of type j' . As described in Section V, such misclassified photons contribute to “invalid” detector-setting choices. The parameter $f_{j \rightarrow j'}$ depends on the choice of what cut-off wavelength λ' we choose to distinguish the photons we call red ($\lambda > \lambda'$) from blue ($\lambda < \lambda'$). It also depends on the emission spectra of the astronomical source. These probabilities can be computed from the atmospheric scattering and absorption, detector quantum efficiencies, and transmission/reflection probabilities of the optics in each detector arm. We define the following quantities, which all are dependent on wavelength:

$N_{\text{source}}(\lambda)$: Number distribution of astronomical photons per wavelength that impinge on the top of Earth’s atmosphere towards the telescope, ignoring effects of the interstellar/intergalactic medium. (This is a good approximation at optical frequencies.)

$N_{\text{in}}(\lambda)$: Number of photons per wavelength that are transmitted through the atmosphere and impinge on the pinhole mirror.

$\rho_{\text{lens}}(\lambda)$: Probability of transmission through the collimating or focusing lens.

$\rho_{\text{det}}(\lambda)$: Probability of detection by the APD (quantum efficiency).

$R(\lambda), B(\lambda)$: Probability of entering the red/blue arm due to the dichroic beamsplitters.

In terms of these quantities, we can compute the overall spectral response of the red/blue arms of the instrument:

$$\begin{aligned} \rho_{\text{blue}} &= B \times \rho_{\text{lens}}^2 \times \rho_{\text{det}} \\ \rho_{\text{red}} &= R \times \rho_{\text{lens}}^2 \times \rho_{\text{det}} \end{aligned}$$

as well as the parameters $f_{j \rightarrow j'}$:

$$f_{b \rightarrow r} = \frac{\int_0^{\lambda'} N_{\text{in}} R d\lambda}{\int_0^{\infty} N_{\text{in}} R d\lambda}, \quad f_{r \rightarrow b} = \frac{\int_{\lambda'}^{\infty} N_{\text{in}} B d\lambda}{\int_0^{\infty} N_{\text{in}} B d\lambda}. \quad (10)$$

For bright stars such as the ones we observe, the quantity $N_{\text{source}}(\lambda)$ is well-approximated by a blackbody [43]. For dim, redshifted quasars, we apply the appropriate Doppler shift to the composite rest-frame spectrum computed in [44]. Once N_{source} is obtained, we compute $N_{\text{in}}(\lambda)$ via the equation

$$N_{\text{in}}/N_{\text{source}} = \rho_{\text{atm}}(\lambda) \exp(-X\tau(\lambda)) \quad (11)$$

where $\rho_{\text{atm}}(\lambda)$ is taken from the atmospheric radiative transfer code MODTRAN [45] and takes into account the Rayleigh scattering and atmospheric absorption at zenith.

In order to correct for off-zenith observations, we insert a factor of $\exp(-X\tau(\lambda))$ where X is the observation airmass and $\tau(\lambda)$ is the optical depth due to Rayleigh scattering. In doing so, we make the approximation that the contribution to $f_{j \rightarrow j'}$ due to the optical density of absorption is negligible compared to Rayleigh scattering. For the quasars listed in Table II, we compute $f_{j \rightarrow j'}$ values in the ranges $0.16\% < f_{b \rightarrow r} < 0.20\%$ and $0.17\% < f_{r \rightarrow b} < 0.23\%$, an order of magnitude better than the values of $f_{j \rightarrow j'}$ achieved with the instrumentation used for the original cosmic Bell experiment in Ref. [1]. We plot in Fig. 7D the products $\rho_{\text{blue}} N_{\text{in}}$ and $\rho_{\text{red}} N_{\text{in}}$, where N_{in} is computed for the quasar PG 1718+481 at an observation altitude of 67 degrees.

VIII. FLUX CALIBRATION WITH HIPPARCOS STARS

We observed a number of different colored stars roughly at zenith. Count rates for these, along with quasars (discussed in Section X) are plotted in Fig. 8 as a function of astronomical V-band magnitude, denoted m_V . The V-band is defined by a broad filter centered at 551 nm with a full width at half max of 88 nm.

To characterize the dark-count rates of the instrument, we close the telescope dome and obstruct its aperture

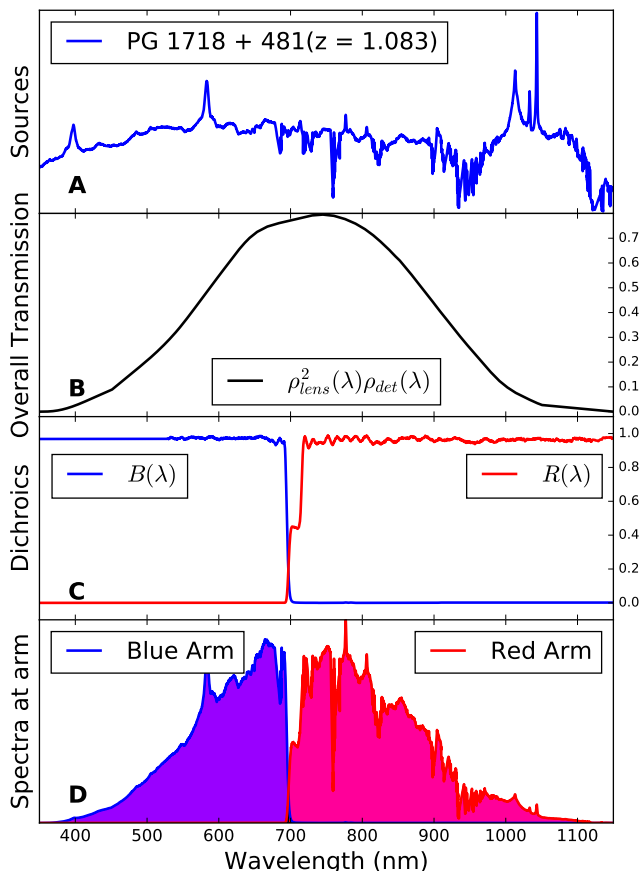


FIG. 7. A: The atmosphere-attenuated spectrum of a typical quasar. B: The cumulative transmission curves of two lenses and the detectors. C: The splitting of photons down the blue/red arms induced by the dichroic beamsplitters. D: The product of curves in A-C gives the effective “filter” at each arm, from which $f_{j \rightarrow j'}$ can be computed.

with a tarp, and measure dark counts for about 500 seconds. We find that the variability in count rates, when integrated over 1 second, is consistent with a Poisson process with variance \sqrt{N} : In the blue arm we see 41 cps, and in the red arm we see 93 cps. A comprehensive list of our star observations is available upon request.

For our telescope and coupling, we find that the astronomical photon flux in counts per second, after subtracting skyglow and dark counts, is given approximately by

$$\log_{10}(\text{count rate}) = 8.12 - (0.363 \pm 0.013)m_V.$$

The deviation from the expected slope of -0.4 is due to detector saturation at count rates higher than $\sim 1 \times 10^5$ Hz.

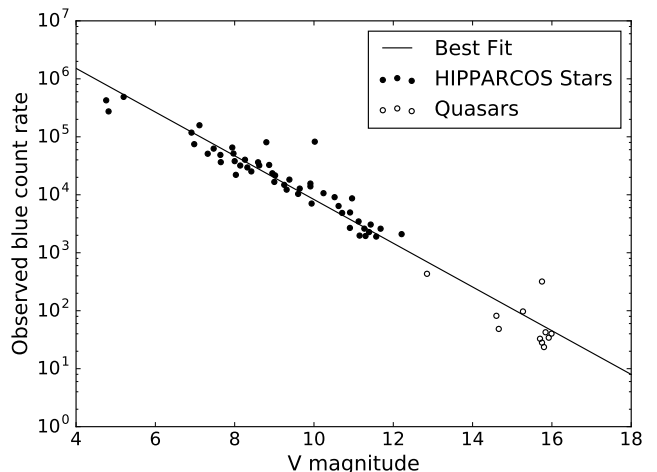


FIG. 8. For 50 bright stars in the HIPPARCOS catalog observed at zenith and eleven high-redshift quasars ($z < 3.911$), we plot the total (red + blue) background-subtracted count rate against the V-band magnitude (551 ± 88 nm). Though the V-magnitude is well into our blue band, it is the only data available for all observed objects and turns out to be a good predictor of the observed photon flux, as seen by the best-fit line that relates the two. We see subtle evidence of detector nonlinearity at high count rates, as discussed in the text.

IX. TIMING CALIBRATION WITH THE CRAB PULSAR

One application of high time-resolution optical detectors in astronomy is to precisely measure the pulsation rate and folded light curve of the Crab Pulsar, whose light curve exhibits a 33 ms periodicity. This is the only source we observed whose photon arrival times have an intrinsically non-random structure on sub-second timescales. By using this stable astronomical clock, we can verify both sub-millisecond and long-term timing stability of our entire system, including the telescope, optics, detectors, time-tagging module, and GPS absolute reference.

Here we report one such folded light curve with our combined red and blue observing band. We observed the Crab Pulsar for one hour on Dec. 21, 2016 (Modified Julian Date [MJD] = 57743) at Table Mountain Observatory and simultaneously recorded a 1 pulse-per-second signal from a TM-4 GPS unit. While the ID801 time-tagging unit has 81 ps relative timing resolution, the GPS unit has 25 ns absolute long-term stability referenced to UTC and 10^{-11} relative stability over one second. The 1 pulse-per-second signal from the GPS provides a more stable frequency reference than the internal clock on the ID801 time-tagging unit and allows for calibration of period measurements.

We determine the period by computing the complex periodogram of our list of detections, defined to be

$$F(T) = \sum_{t \in \text{all time tags}} \exp\left(2\pi i \frac{t}{T}\right)$$

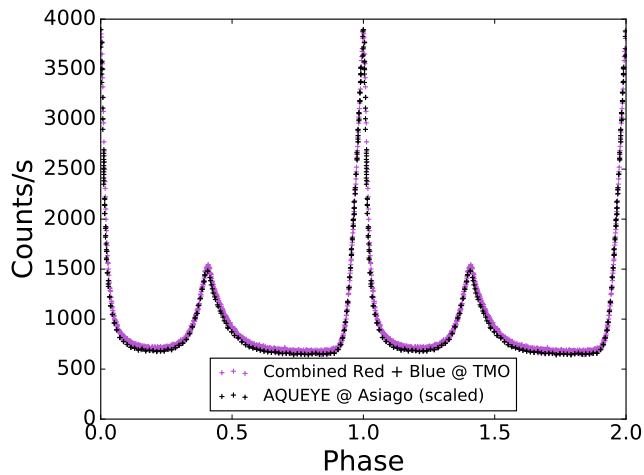


FIG. 9. We plot two full periods of the folded light curve of the Crab Pulsar, in our combined observation band, spanning from roughly 350 nm – 1150 nm. The individual detection events are placed into 256 time bins of equal length. We compare our measured light curve to that of the high time-resolution instrument Aqueye [47], which has a similar observing band to our combined red and blue observing band. The Aqueye data has been shifted in time, scaled, and given a DC offset. We observe excellent agreement in the pulse profile. Our best-fit period T was determined by considering the periodogram of each photon detection over an hour-long observation. The y-axis has been normalized such that the weighted average of the light curve adds up to the average observed photon flux in counts per second. The \sqrt{N} error bars in each individual time-bin are too small to be seen.

and observe that numerically maximizing $|F(T)|$ over T gives us the period of the pulsar. We correct for slow drifts in the time-tagging unit by using the GPS’s one-pulse-per-second (1pps). We correct for the radial velocity of Earth with respect to the pulsar. We obtain an estimate of the period in agreement with the Jodrell Bank ephemeris [46] to within a few parts in 10^7 , as shown in Table I.

At this level of precision, several sources of error may be significant. Finite-length sampling effects give a fundamental uncertainty $\Delta T_{\text{sampling}}$ in the period as determined by our periodogram method. Using the sampling theorem, we estimate the size of this effect to be $\Delta T_{\text{sampling}}/T \sim \text{Period}/\text{Duration} \sim 10^{-8}$. In addition, our Doppler correction did not correct for the earth’s variable radial velocity as it rotates on its axis, which induces a sinusoidal variation in the period T over the entire duration of our observation with a daily amplitude of $\Delta T/T \sim 10^{-7}$.

Once the best-fit period is obtained, we histogram our photon counts into 256 periodic time bins. The overall DC offset is a reflection of the dark counts, sky glow, as well as the light from the pulsar’s surrounding nebula. The folded light curve is shown in Fig. 9.

X. OBSERVATION OF QUASARS

We recorded photon count rates from a number of quasars, with V band magnitudes ranging from 12.9 to 16, and redshifts up to $z = 3.911$. Light travel times τ are calculated from the maximally-constrained cosmological parameters from the Planck satellite [48]. The two most distant quasars we observed emitted their light over 12 billion years ago, to be compared with the 13.8 billion-year age of the universe. A summary of our quasar observations, and two measures quantifying the physical and information-theoretic predictability of bits ($p^{(i)}$ and I) are presented in Table II.

XI. QUALITY OF RANDOMNESS

In addition to quantifying the fraction of valid runs as was done in Ref. [1], we may assess the quality of randomness statistically to yield a measure of predictability. The NIST Statistical Test Suite [42] provides a device-independent statistical approach to evaluate the quality of the output of any random-number generator given a sufficiently large number of bits. When using timestamps to generate random bits based on whether photons arrive on an even or odd nanosecond, we find that our random numbers pass the NIST test suite, consistent with the findings in Ref. [5]. When using photon colors to generate random bits, our data fail the NIST tests, largely due to the existence of an overall bias in red-blue count rates.

To quantify imperfect statistical randomness in a bit-stream, we may consider the mutual information between a moving window of m bits and the $(m+1)$ th bit, which we denote as $I(m; m+1)$. If each bit were truly independent, this mutual information would be zero, even if the probability to get a 0 or 1 was not 50%. To define $I(m; m+1)$, let \mathcal{X}_m denote the set of all length- m binary strings, and let $p(x)$ be the probability that an m -bit string within our bitstream is $x \in \mathcal{X}_m$. Similarly, let $p(y)$ be the probability that the next bit is $y \in \{0, 1\}$. If we define $p(x, y)$ to be the probability that a string of $m+1$ bits are x followed by y , then the mutual information in our data is defined to be

$$I(m; m+1) = \sum_{x \in \mathcal{X}_m} \sum_{y \in \{0, 1\}} p(x, y) \times \log_2 \left(\frac{p(x, y)}{p(x)p(y)} \right). \quad (12)$$

Note that if the next bit is independent of the m bits preceding it, then $p(x, y) = p(x)p(y)$ and the mutual information vanishes.

Estimating the true mutual information in a sample of length N , denoted $I_N(m; m+1)$, by using experimental estimates of the probabilities $p(x, y)$, $p(x)$, and $p(y)$ is unreliable. Statistical fluctuations in the finite-sample estimates $\hat{p}(x, y)$, $\hat{p}(x)$, and $\hat{p}(y)$ of these probabilities causes the amount of mutual information in the dataset

MJD	T (ms)	Discrepancy ($\Delta T/T$)	Notes
57743	33.730283	—	Jodrell Bank ephemeris (interpolated)
57743	33.729767	-1.9×10^{-5}	Using ID801 internal clock (obs.)
57743	33.730654	$+1.1 \times 10^{-5}$	Clocked to GPS reference (obs.)
57743	33.730290	$+2.8 \times 10^{-7}$	Corrected for relative velocity ($v_r = -3067$ m/s)

TABLE I. Using Jodrell Bank’s monthly measurement of both the pulsar period and the period derivative [46], we can compute the expected pulsar period (T) on our observation date (specified by Modified Julian Date, MJD). As expected, our measurements of the period are closer to the Jodrell Bank prediction when we use an external frequency reference, and when we correct for the radial velocity of the Earth with respect to the Crab pulsar as it moves around the Sun.

Name	Redshift (z)	τ (Gyr)	B	V	blue (cps)	red (cps)	valid fraction $q^{(i)}$	max info $I \times 10^4$
3C 273	0.173	2.219	13.05	12.85	672	1900	0.884	87.8
HS 2154+2228	1.29	8.963	15.2	15.30	227	503	0.774	9.91
MARK 813	0.111	1.484	15.42	15.27	193	633	0.703	7.62
PG 1718+481	1.083	8.271	15.33	14.6	176	473	0.682	3.07
APM 08279+5255	3.911	12.225	19.2	15.2	684	1070	0.647	5.39
PG1634+706	1.337	9.101	14.9	14.66	121	285	0.572	3.38
B1422+231	3.62	12.074	16.77	15.84	123	358	0.507	4.22
HS 1603+3820	2.54	11.234	16.37	15.99	121	326	0.501	4.78
J1521+5202	2.208	10.833	16.02	15.7	106	309	0.476	2.39
87 GB 19483+5033	1.929	10.409	unknown	15.5	98	241	0.464	0.32
PG 1247+268	2.048	10.601	16.12	15.92	111	333	0.453	2.92
HS 1626+6433	2.32	10.979	unknown	15.8	87	213	0.398	1.81

TABLE II. A list of quasars observed, their corresponding redshifts z , and light travel times τ . We report their B and V magnitudes from the SIMBAD Astronomical Database and our observed 75th percentile count rates. The table is sorted by the fraction of valid settings $q^{(i)}$ for each quasar observation, based on both off-target counts measured at each observation’s airmass and rates for quasar photons to go the wrong way through our imperfect dichroics calculated from each quasar’s emission spectrum. Predictability, as measured by $I = \max_m I_N(m; m+1)$, is the small mutual information we measured in each quasar’s bitstream and corresponds to a negligible reduction in $q^{(i)}$. Even using a small (1 m) telescope at a light-polluted Los Angeles observing site, we find that the first quasar (3C 273) paired with either of the next two would yield $q^{\text{Alice}} + q^{\text{Bob}}$ in excess of the limit set by Eq. (4) for addressing the freedom-of-choice loophole.

to be overestimated if we simply “plug in” the experimental probability estimates \hat{p} into Eq. (12), which takes as input the true probabilities p . We denote this biased estimator by $\hat{I}_N(m; m+1)$. However, in the limit that the dataset is large ($N \gg 1$), and if m is fixed, the amount of positive bias in the estimated mutual information $\hat{I}_N(m; m+1)$ is dependent only on N and can be represented as a perturbation away from the true mutual information $I(m; m+1)$. To construct an unbiased estimator, we adopt the ansatz [49]

$$\hat{I}_N(m; m+1) = I(m; m+1) + \frac{a}{N} + \frac{b}{N^2}, \quad (13)$$

where $I(m; m+1)$, a , and b are fixed, unknown constants. To determine these constants, we first compute $\hat{I}_N(m; m+1)$ for the entire dataset. By splitting the dataset into 2 chunks of size $N/2$, we may estimate $\hat{I}_{N/2}(m; m+1)$ by averaging the naive estimate from both chunks. Repeating this procedure for 4 chunks of size $N/4$ gives us a system of three equations linear in the unknowns $I(m; m+1)$, a , and b .

From this procedure, we compute an unbiased estimate of the mutual information in the bits we generate when taking on-quasar data as well as data taken when pointing at the sky slightly off-target. We compute

$I(m; m+1)$ for $m = 1, 2, \dots, 6$ lookback bits on datasets of length $N > 2^{16}$. To determine whether our estimates are consistent with zero mutual information, we compare our estimates of $I_N(m; m+1)$ against fifty simulated datasets, each with the same length and the same red/blue bias but with no mutual information. Examples of a quasar bitstream with almost no mutual information (PG 1718+481) and a quasar bitstream with nonzero mutual information (3C 273) are shown in Fig. 10.

For the quasars in Table II, we observe that the random bits generated from colors in 8 out of 12 datasets exhibit mutual information that is statistically significantly different from zero, though still very small. This hints at the possibility of some nontrivial structure in the data which may be induced by physical effects or systematic error. In 11/12 datasets, the maximum information $I = \max_m I(m; m+1)$ is less than 0.001, while for the exceptionally bright quasar 3C 273 ($V = 12.9$), we measure $I \approx 0.009$. One way to realize a mutual information of 0.001 is to have one in every 1000 bits be a deterministic function of the previous few bits instead of being random. Even in the worst case of 0.009, the amount of predictability is only increased negligibly compared to the effect from skyglow, and is well below the threshold needed to address the freedom-of-choice loophole in a Bell test.

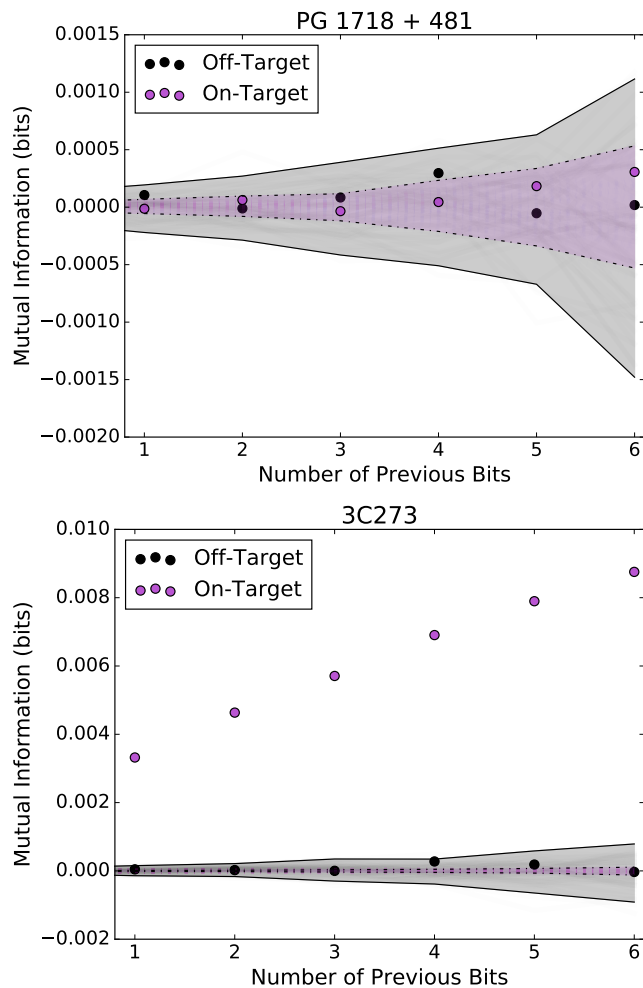


FIG. 10. The experimental estimate of the mutual information between a bit and the m bits preceding it, for $m = 1, \dots, 6$, for two different quasars. To check for nonzero mutual information in our on-target data (open circles, purple online) and off-target data (closed circles, black), we estimate the mutual information of 50 simulated datasets with the same length and the same red-blue bias with no mutual information, and shade 2σ error bars about the mean. Error bars for on-target and off-target data are denoted with dashed and dotted lines respectively. For the quasar PG1718+481, we find that the experimentally observed mutual information in the on-target as well as the off-target data is consistent with zero, while for the exceptionally bright quasar 3C 273, the on-target data deviates significantly from zero.

For example, in the recent cosmic Bell experiment [1], violations of the Bell-CHSH inequality were found with high statistical significance (>7 standard deviations) for an experiment involving $\sim 10^5$ detected pairs of entangled photons, even with excess predictability in each arm of each detector of order $p^{(i)} \sim 0.1$.

Upon examining the experimental probability estimates $\hat{p}(x, y)$ that went into the mutual information calculation, we identified two systematic sources of non-randomness, both of which are exacerbated at high

fluxes. The first mechanism for non-randomness is detector saturation. After a detection, the detector has a 420 ns deadtime window during which a detection is improbable. Hence for sufficiently high count rates (such as those experienced when observing stars), it is much more likely to observe a blue photon following a red one and vice versa than multiple photons of the same color in a row. While we see this effect in our calibration data with HIPPARCOS stars, the count rates necessary for this effect to be important ($10^5 - 10^6$ counts per second) far exceed what is observed with quasars. These are eliminated by imposing the same deadtime window in the other channel and removing (in real time or in post-processing) any detection that is within the deadtime of any previous detection from either channel.

The second mechanism is a consequence of imperfect alignment combined with random atmospheric seeing. Within our device’s pinhole, we know there exists a “sweet spot” for optimal coupling to the blue detector, and a slightly different sweet spot for optimal alignment with the red detector. As the image of the quasar twinkles within the pinhole on timescales of milliseconds, its instantaneous scintillation pattern overlaps differently with these sweet spots. The result is that on scales of less than a millisecond, the conditional probability $p(x \rightarrow y)$ of receiving detection y given previous detections x is higher than the average probability $p(y)$. For example, for quasar 3C273 we see $p(10111 \rightarrow 1) = p(101111)/p(10111) > p(1)$.

Since atmospheric seeing is a consequence of random atmospheric turbulence, it is a potential source of local influences on astronomical randomness. It can be mitigated by careful characterization of the optical alignment of the system, making sure that the sweet spots of both detector arms overlap to the greatest extent possible, and observing under calm atmospheric conditions. For a larger telescope in a darker location where the signal to background ratio is higher, this would be a relatively larger effect on the fraction of valid runs.

XII. CONCLUSION

Building on the design and implementation of astronomical random-number generators in the recent cosmic Bell experiment [1], we have demonstrated the capabilities of a telescope instrument that can output a time-tagged bitstream of random bits based on the detection of single photons from astronomical sources with tens of nanoseconds of latency. We have further demonstrated its feasibility as a source of random settings for such applications as testing foundational questions in quantum mechanics, including asymptotically closing the freedom-of-choice loophole in tests of Bell’s inequality, and conducting a cosmic-scale delayed-choice quantum-eraser experiment. Beyond such foundational tests, astronomical sources of random numbers could also be of significant use in quantum-cryptographic applications akin to those

described in Refs. [5, 26–31].

Other interesting applications of this device may be found in high time-resolution astrophysics. For example, it might be possible to indirectly detect gravitational waves and thereby perform tests of general relativity with the careful observation of several optical pulsars using future versions of our instrument and larger telescopes, complementing approaches described in Refs. [50–54].

ACKNOWLEDGEMENTS

We are grateful to members of the cosmic Bell collaboration for sharing ideas and suggestions regarding the instrument and analyses discussed here, and for helpful comments on the manuscript, especially Johannes Handsteiner, Dominik Rauch, Thomas Scheidl, Bo Liu, and

Anton Zeilinger. Heath Rhoades and the other JPL staff at Table Mountain were invaluable for observations. We also acknowledge Michael J. W. Hall for helpful discussions, and Beili Hu and Sophia Harris for providing valuable feedback on the manuscript. Funding for hardware and support for CL and AB was provided by JG’s Harvey Mudd startup. This research was carried out partly at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration and funded through the internal Research and Technology Development program. This work was also supported in part by NSF INSPiRE Grant No. PHY-1541160. Portions of this work were conducted in MIT’s Center for Theoretical Physics and supported in part by the U.S. Department of Energy under Contract No. de-sc0012567.

-
- [1] J. Handsteiner, A. S. Friedman, D. Rauch, J. Gallicchio, B. Liu, H. Hosp, J. Kofler, D. Bricher, M. Fink, C. Leung, et al., “Cosmic Bell test: Measurement settings from Milky Way stars,” *Phys. Rev. Lett.* **118**, 060401 (2017), [arXiv:1611.06985 \[quant-ph\]](#).
- [2] T. Scheidl, R. Ursin, J. Kofler, S. Ramelow, X.-S. Ma, T. Herbst, L. Ratschbacher, A. Fedrizzi, N. K. Langford, T. Jennewein, et al., “Violation of Local Realism with Freedom of Choice,” *Proc. Natl. Acad. Sci. USA* **107**, 19708–19713 (2010), [arXiv:0811.3129 \[quant-ph\]](#).
- [3] X.-S. Ma, J. Kofler, A. Qarry, N. Tetik, T. Scheidl, R. Ursin, S. Ramelow, T. Herbst, L. Ratschbacher, A. Fedrizzi, et al., “Quantum Erasure with Causally Disconnected Choice,” *Proc. Natl. Acad. Sci. USA* **110**, 1221–1226 (2013), [arXiv:1206.6578 \[quant-ph\]](#).
- [4] J. Gallicchio, A. S. Friedman, and D. I. Kaiser, “Testing Bell’s Inequality with Cosmic Photons: Closing the Setting-Independence Loophole,” *Phys. Rev. Lett.* **112**, 110405 (2014), [arXiv:1310.3288 \[quant-ph\]](#).
- [5] C. Wu, B. Bai, Y. Liu, X. Zhang, M. Yang, Y. Cao, J. Wang, S. Zhang, H. Zhou, X. Shi, et al., “Random Number Generation with Cosmic Photons,” *Phys. Rev. Lett.* **118**, 140402 (2017), [arXiv:1611.07126 \[quant-ph\]](#).
- [6] J. S. Bell, “On the Einstein Podolsky Rosen paradox,” *Physics* **1**, 195–200 (1964).
- [7] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, “Bell Nonlocality,” *Rev. Mod. Phys.* **86**, 419–478 (2014), [arXiv:1303.2849 \[quant-ph\]](#).
- [8] J.-Å. Larsson, “Loopholes in Bell Inequality Tests of Local Realism,” *J. Phys. A* **47**, 424003 (2014), [arXiv:1407.0363 \[quant-ph\]](#).
- [9] J. Kofler, M. Giustina, J.-Å. Larsson, and M. W. Mitchell, “Requirements for a Loophole-Free Photonic Bell Test using Imperfect Setting Generators,” *Phys. Rev. A* **93**, 032115 (2016), [arXiv:1411.4787 \[quant-ph\]](#).
- [10] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, et al., “Loophole-Free Bell Inequality Violation Using Electron Spins Separated by 1.3 Kilometres,” *Nature (London)* **526**, 682–686 (2015), [arXiv:1508.05949 \[quant-ph\]](#).
- [11] M. Giustina, M. A. M. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J.-Å. Larsson, C. Abellán, et al., “Significant-Loophole-Free Test of Bell’s Theorem with Entangled Photons,” *Phys. Rev. Lett.* **115**, 250401 (2015), [arXiv:1511.03190 \[quant-ph\]](#).
- [12] L. K. Shalm, E. Meyer-Scott, B. G. Christensen, P. Bierhorst, M. A. Wayne, M. J. Stevens, T. Gerrits, S. Glancy, D. R. Hamel, M. S. Allman, et al., “Strong Loophole-Free Test of Local Realism*,” *Phys. Rev. Lett.* **115**, 250402 (2015), [arXiv:1511.03189 \[quant-ph\]](#).
- [13] W. Rosenfeld, D. Burchardt, R. Garthoff, K. Redeker, N. Ortegel, M. Rau, and H. Weinfurter, “Event-Ready Bell-Test Using Entangled Atoms Simultaneously Closing Detection and Locality Loopholes,” *ArXiv e-prints* (2016), [arXiv:1611.04604 \[quant-ph\]](#).
- [14] M. J. W. Hall, “Local Deterministic Model of Singlet State Correlations Based on Relaxing Measurement Independence,” *Phys. Rev. Lett.* **105**, 250404 (2010), [arXiv:1007.5518 \[quant-ph\]](#).
- [15] M. J. W. Hall, “Relaxed Bell Inequalities and Kochen-Specker theorems,” *Phys. Rev. A* **84**, 022102 (2011), [arXiv:1102.4467 \[quant-ph\]](#).
- [16] J. Barrett and N. Gisin, “How Much Measurement Independence is Needed to Demonstrate Nonlocality?” *Phys. Rev. Lett.* **106**, 100406 (2011), [arXiv:1008.3612 \[quant-ph\]](#).
- [17] M. Banik, M. Rajjak Gazi, S. Das, A. Rai, and S. Kunkri, “Optimal Free Will on One Side in Reproducing the Singlet Correlation,” *J. Phys. A* **45**, 205301 (2012), [arXiv:1204.3835 \[quant-ph\]](#).
- [18] G. Pütz, D. Rosset, T. J. Barnea, Y.-C. Liang, and N. Gisin, “Arbitrarily Small Amount of Measurement Independence Is Sufficient to Manifest Quantum Nonlocality,” *Phys. Rev. Lett.* **113**, 190402 (2014), [arXiv:1407.5634 \[quant-ph\]](#).
- [19] G. Pütz and N. Gisin, “Measurement Dependent Locality,” *New J. Phys.* **18**, 055006 (2016), [arXiv:1510.09087 \[quant-ph\]](#).
- [20] M. J. W. Hall, “The significance of measurement independence for Bell inequalities and locality,” in *At the*

- Frontier of Spacetime – Scalar-Tensor Theory, Bell’s Inequality, Mach’s Principle, Exotic Smoothness*, edited by T. Asselmeyer-Maluga (Springer, Switzerland, 2016) Chap. 11, pp. 189–204, [arXiv:1511.00729 \[quant-ph\]](#).
- [21] S. Pironio, “Random ‘Choices’ and the Locality Loop-hole,” ArXiv e-prints (2015), [arXiv:1510.00248 \[quant-ph\]](#).
- [22] J. A. W. Wheeler, “The ‘past’ and the ‘delayed-choice’ double-slit experiment,” in *Mathematical Foundations of Quantum Theory*, edited by A. R. Marlow (Academic Press, New York, 1978) pp. 9–48.
- [23] J. A. W. Wheeler, “Law without law,” in *Quantum Theory and Measurement*, edited by J. A. W. Wheeler and W. H. Zurek (Princeton University Press, 1983) pp. 182–213.
- [24] W. A. Miller and J. A. Wheeler, “Delayed-choice experiments and Bohr’s elementary quantum phenomenon,” in *Proceedings of the International Symposium Foundations of Quantum Mechanics in the Light of New Technology* edited by S. Kamefuchi (Physical Society of Japan, 1984) pp. 140–152.
- [25] X.-S. Ma, J. Kofler, and A. Zeilinger, “Delayed-choice gedanken experiments and their realizations,” *Rev. Mod. Phys.* **88**, 015005 (2016), [arXiv:1407.2930 \[quant-ph\]](#).
- [26] J. Barrett, L. Hardy, and A. Kent, “No Signaling and Quantum Key Distribution,” *Phys. Rev. Lett.* **95**, 010503 (2005), [quant-ph/0405101](#).
- [27] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani, “Device-independent quantum key distribution secure against collective attacks,” *New J. Phys.* **11**, 045021 (2009), [arXiv:0903.4460 \[quant-ph\]](#).
- [28] S. Pironio, A. Acín, S. Massar, A. B. de La Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, et al., “Random numbers certified by Bell’s theorem,” *Nature (London)* **464**, 1021–1024 (2010), [arXiv:0911.3427 \[quant-ph\]](#).
- [29] R. Colbeck and R. Renner, “Free randomness can be amplified,” *Nature Phys.* **8**, 450–454 (2012), [arXiv:1105.3195 \[quant-ph\]](#).
- [30] R. Gallego, L. Masanes, G. de la Torre, C. Dhara, L. Aolita, and A. Acín, “Full randomness from arbitrarily deterministic events,” *Nature Comm.* **4**, 2654 (2013), [arXiv:1210.6514 \[quant-ph\]](#).
- [31] U. Vazirani and T. Vidick, “Fully Device-Independent Quantum Key Distribution,” *Phys. Rev. Lett.* **113**, 140501 (2014).
- [32] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, “Proposed experiment to test local hidden-variable theories,” *Phys. Rev. Lett.* **23**, 880 (1969).
- [33] B. Tsirelson, “Quantum Bell-type inequalities,” *Hadronic Journal Supplement* **8**, 329–345 (1993).
- [34] V. Jacques, E. Wu, F. Grosshans, F. Treussart, P. Grangier, A. Aspect, and J.-F. Roch, “Delayed-Choice Test of Quantum Complementarity with Interfering Single Photons,” *Phys. Rev. Lett.* **100**, 220402 (2008), [arXiv:0801.0979 \[quant-ph\]](#).
- [35] J. C. Owens, “Optical refractive index of air: Dependence on pressure, temperature and composition,” *Applied optics* **6**, 51–59 (1967).
- [36] P. J. E. Peebles, *Principles of Physical Cosmology* (Princeton University Press, 1993).
- [37] S. Weinberg, *Cosmology* (Oxford University Press, 2008).
- [38] R. D. Blandford and R. Narayan, “Cosmological applications of gravitational lensing,” *Ann. Rev. Astron. Astrophys.* **30**, 311–358 (1992).
- [39] A. Rogers, “Frequency-dependent effects of gravitational lensing within plasma,” *Mon. Not. R. Astron. Soc.* **451**, 4536–4544 (2015), [arXiv:1505.06790 \[gr-qc\]](#).
- [40] J. S. Bell, *Speakable and Unspeakable in Quantum Mechanics* (Cambridge University Press, 1987).
- [41] J. W. M. Bush, “Pilot-wave hydrodynamics,” *Ann. Rev. Fluid Mech.* **47**, 269–292 (2015).
- [42] L. E. Bassham III, A. L. Rukhin, J. Soto, J. R. Nechvatal, M. E. Smid, E. B. Barker, S. D. Leigh, M. Levenson, M. Vangel, D. L. Banks, et al., “Statistical test suite for random and pseudorandom number generators for cryptographic applications,” *Special Publication (NIST SP) 800-22 Rev 1a* (2010).
- [43] F. J. Ballesteros, “New Insights into Black Bodies,” *EPL (Europhysics Letters)* **97**, 34008 (2012), [arXiv:1201.1809 \[astro-ph.IM\]](#).
- [44] D. E. Vanden Berk, G. T. Richards, A. Bauer, M. A. Strauss, D. P. Schneider, T. M. Heckman, D. G. York, P. B. Hall, X. Fan, G. R. Knapp, et al., “Composite Quasar Spectra from the Sloan Digital Sky Survey,” *Astron. J.* **122**, 549–564 (2001), [astro-ph/0105231](#).
- [45] A. Berk, P. Conforti, R. Kennett, T. Perkins, F. Hawes, and J. van den Bosch, “MODTRAN6: a Major Upgrade of the MODTRAN Radiative Transfer Code,” in *Algorithms and Technologies for Multispectral, Hyperspectral, and Ultraspectral Imagery XX*, Proc. SPIE, Vol. 9088 (2014) p. 90880H.
- [46] A. G. Lyne, R. S. Pritchard, and F. G. Smith, “23 years of Crab pulsar rotational history,” *Mon. Not. R. Astron. Soc.* **265**, 1003–1012 (1993).
- [47] C. Germanà, L. Zampieri, C. Barbieri, G. Naletto, A. Čadež, M. Calvani, M. Barbieri, I. Capraro, A. Di Paola, C. Facchinetti, et al., “Aqueye Optical Observations of the Crab Nebula Pulsar,” *Astron. Astrophys.* **548**, A47 (2012), [arXiv:1210.1796 \[astro-ph.HE\]](#).
- [48] Planck Collaboration, P. A. R. Ade, et al., “Planck 2015 results. XIII. Cosmological parameters,” *Astron. Astrophys.* **594**, A13 (2016), [arXiv:1502.01589](#).
- [49] A. Treves and S. Panzeri, “The upward bias in measures of information derived from limited data samples,” *Neural Computation* **7**, 399–407 (1995).
- [50] G. Hobbs, “The Parkes Pulsar Timing Array,” *Class. Quant. Grav.* **30**, 224007 (2013), [arXiv:1307.2629 \[astro-ph.IM\]](#).
- [51] M. A. McLaughlin, “The North American Nanohertz Observatory for gravitational waves,” *Class. Quant. Grav.* **30**, 224008 (2013), [arXiv:1310.0758 \[astro-ph.IM\]](#).
- [52] M. Kramer and D. J. Champion, “The European Pulsar Timing Array and the Large European Array for Pulsars,” *Class. Quant. Grav.* **30**, 224009 (2013).
- [53] R. N. Manchester, “The International Pulsar Timing Array,” *Class. Quant. Grav.* **30**, 224010 (2013), [arXiv:1309.7392 \[astro-ph.IM\]](#).
- [54] T. J. W. Lazio, “The Square Kilometre Array pulsar timing array,” *Class. Quant. Grav.* **30**, 224011 (2013).