



# Parity-based, bias-free optical quantum random number generation with min-entropy estimation

MATHEW R. COLEMAN, KAYLIN G. INGALLS, JOHN T. KAVULICH, SAWYER J. KEMMERLY, NICOLAS C. SALINAS, EFRAIN VENEGAS RAMIREZ, AND MAXIMILIAN SCHLOSSHAUER\* 

Department of Physics, University of Portland, 5000 North Willamette Boulevard, Portland, Oregon 97203, USA

\*Corresponding author: schlossh@up.edu

Received 6 March 2020; revised 7 May 2020; accepted 27 May 2020; posted 28 May 2020 (Doc. ID 392286); published 23 June 2020

We describe the generation of sequences of random bits from the parity of photon counts produced by polarization measurements on a polarization-entangled state. The resulting sequences are bias free, pass the applicable tests in the NIST battery of statistical randomness tests, and are shown to be Borel normal, without the need for experimental calibration stages or postprocessing of the output. Because the photon counts are produced in the course of a measurement of the violation of the Clauser–Horne–Shimony–Holt inequality, we are able to concurrently verify the nonclassical nature of the photon statistics and estimate a lower bound on the min-entropy of the bit-generating source. The rate of bit production in our experiment is around 13 bits/s. © 2020 Optical Society of America

<https://doi.org/10.1364/JOSAB.392286>

Note: The following material may be protected by copyright law (Title 17, U.S. Code)

## 1. INTRODUCTION

Random numbers constitute a valuable resource [1], with applications ranging from simulations of complex systems [2,3] and cryptography [4] to fundamental quantum experiments [5] and information technology [1]. A quantum random number generator (QRNG) [6] produces bits from an indeterministic quantum process. A typical approach consists of performing measurements on quantum systems prepared in a coherent superposition state. This approach makes use of the fact that the outcomes of such measurements are fundamentally unpredictable [7]. Optical systems based on quantum properties of photons are particularly popular due to the ease with which photons can be produced, manipulated, and measured [6]. There are many different types of such optical QRNGs, distinguished by the particular kind of physical principle and measurement exploited in the generation of bits, such as branching paths [8], photon-number statistics [9,10], time-of-arrival statistics [11,12], vacuum fluctuations [13–15], and Raman scattering [16]. Systems based on the detection of single photons have shown especially high bit rates and efficiencies [8–12]. They have also enabled a concurrent verification of quantum randomness and security in terms of bounds on the source min-entropy obtained from quantum state tomography [17,18], prepare-and-measure protocols [19], and violations of Bell inequalities [20–23]. A paradigmatic type of a single-photon QRNG is the branching-path generator [8]. Such a generator may be realized by letting single photons, each prepared in a superposition state  $(|H\rangle + e^{i\phi}|V\rangle)/\sqrt{2}$ , traverse a polarizing beam splitter, followed by their detection at the two outputs of the beam splitter.

Each such polarization measurement in the  $HV$  basis then produces a single random bit.

From a fundamental point of view, the fact that a QRNG generates bits from a physically random process makes it superior to a pseudorandom number generator (PRNG). A PRNG uses a deterministic algorithm fed with an initial seed, and thus its output is by definition computable [24]. In contrast, for a QRNG, the value indefiniteness implied by the Kochen–Specker theorem [25] can guarantee the incomputability of the output [26,27]. One can also exploit the properties of quantum entanglement to experimentally certify the randomness and privacy (and hence security) of the output of a QRNG [20–22]. While these are striking advantages over PRNGs, practical realizations of QRNGs exhibit problems of their own [6]. In particular, they tend to be susceptible to substantial bias and correlation effects that may detrimentally affect the quality of the output from the point of view of statistical and algorithmic randomness [28–30]. In the photonic scenario just described, bias may arise from sources such as imperfect state preparation with nonequalized amplitudes, a polarizing beam splitter that does not reliably separate  $H$  and  $V$  polarizations, and imbalanced detectors. Correlations may be caused, for example, by dead-time and afterpulsing effects in the detectors [29,31,32]. In practical implementations, these imperfections often have a significant influence and can be difficult to avoid [6]. Mitigation of bias effects generally requires the application of an unbiasing algorithm during postprocessing of the output [6], and some optical QRNGs also include explicit calibration [8] and feedback [29] stages to fine-tune and balance detector efficiencies, coupling ratios of beam splitters, and other parameters.

Here we describe a single-photon experiment in which bias is avoided by using the parity of accumulated photon counts to produce the random bits. In this way, our QRNG does not require calibration or postprocessing to generate random numbers that, as we will show, pass both all applicable statistical randomness tests of the NIST suite [33] and a test of Borel normality [24,34]. Borel normality is an important criterion as it taps the realm of algorithmic (rather than statistical) randomness, an area of particular interest for QRNGs. Yet there exist only a few studies to date that have used Borel normality for testing QRNGs and probing the kind of incomputability and algorithmic randomness that in principle sets them apart from PRNGs [28–30].

In the photonic context, the approach of using the parity of photon counts to produce random numbers was previously explored in an experiment by Fürst *et al.* [9], in which attenuated LED light was detected with a photomultiplier tube. This setup also became the basis of the commercial generator quRNG [35]. Our own experiment uses a rather different, quantum-optical setup, which is based on polarization measurements on entangled photon pairs generated from spontaneous parametric downconversion. A chief motivation for using this kind of setup is that it enables us to concurrently measure a lower bound on the min-entropy of the source and, in this way, to perform an active assessment of the presence of quantum randomness. We do this in two complementary ways, namely, (i) by tomographically measuring the two-photon quantum state and using a theoretical result derived by Fiorentino *et al.* [17,18], and (ii) by measuring the violation of the Clauser–Horne–Shimony–Holt inequality [36] and applying to it a theorem of Pironio *et al.* [20].

This integration of parity-based single-photon quantum random generation with a verification of min-entropy and quantum randomness via measurements on entangled states distinguishes our experiment from other optical QRNGs that produce bias-free random numbers without postprocessing, such as those described in Refs. [9,11,15,37–40]. Our experiment also provides full control over the preparation of the quantum states and measurement settings, and it does not require any time-tagging of individual photon events. This last property is a consequence of the fact that only the number of registered photons per counting interval is needed to obtain a random bit, and likewise, the randomness verification via measurements of the quantum state and the CHSH inequality requires the observation only of the statistics of photon counts.

Our paper is organized as follows. In Section 2, we briefly review the estimation of the source min-entropy from quantum state tomography and from violations of the CHSH inequality. In Section 3, we describe our experimental setup and generation of the random bits. In Section 4, we report the measured bounds on the source min-entropy and describe the results of randomness testing performed on the generated bit sequences. We offer concluding remarks in Section 5.

## 2. MIN-ENTROPY ESTIMATION

In our experiment, polarization measurements on the prepared two-photon state serve as a generator of randomness and thus of entropy. We can estimate the entropy produced by this

source in terms of the min-entropy [41]. The min-entropy may be thought of as quantifying the effectiveness of any strategy that tries to guess, at first attempt, the most likely output of the source. In the quantum setting, there are two particularly important methods for estimating the source min-entropy. The first is the use of a measurement of the quantum state to quantify the amount of coherence and bias between the two state components that define the randomness-generating measurement outcomes [17,18,42]. The second method uses the connection between violations of the CHSH inequality and the nonclassicality of the output [20–22]. We will use both of these methods, and below shall briefly describe them in turn; for more details, see Refs. [17,18,20–22,42].

For each of the two methods, we obtain a lower bound on the source min-entropy per measurement event. If we were to directly generate a sequence of random bits from those individual events (with each event producing one bit), then according to the meaning of the min-entropy [43], the min-entropy bound would also give the minimum number of uniform (and secure [17,18,20]) random bits that can be extracted from this sequence. In our case, however, we do not translate the measurement events individually into bits, but instead produce the bits from the parity of the number of many such accumulated events. Therefore, the numerical value of the min-entropy bound cannot be applied to measuring the extractability of randomness from our sequences of bits. Indeed this is not surprising, since the min-entropy quantifies the randomness of the process, which is that of individual quantum measurements. Nonetheless, what measuring a nonzero min-entropy bound accomplishes as far as our parity-generated sequences are concerned is a confirmation of the presence of quantum randomness in the measured photon counts [17,18,20–22,42]. Since our random numbers are produced from a property of the measured photon events—namely, the parity of their numbers—those bits must also contain elements of quantum randomness. The presence of quantum randomness also relates to the privacy and security of the output: it guarantees that the polarization measurements done by one party (Alice) produce fresh randomness even if an adversary (Eve) has prepared the state Alice is measuring, or if Alice’s photons are quantum-correlated with Eve’s [17,18].

For the min-entropy bound obtained from knowledge of the quantum state, we make use of a result by Fiorentino *et al.* [17,18], who showed that for photons in a known state  $\hat{\rho}$ , the min-entropy  $H_\infty(\hat{\rho})$  per  $HV$  measurement is bounded from below by

$$H_\infty^{\min}(\hat{\rho}) = -\log_2 \left( \frac{1 + \sqrt{1 - 4C^2}}{2} \right), \quad (1)$$

where  $C$  is the magnitude of the off-diagonal elements of  $\hat{\rho}$  expressed in the  $HV$  basis. In Ref. [42], we discuss the connection underlying Eq. (1) between the off-diagonal elements and quantum randomness. To apply Eq. (1) to our experiment, we take the tomographically reconstructed density matrix for the entangled two-photon state, restrict it to the subspace spanned by  $|H\rangle|H\rangle$  and  $|V\rangle|V\rangle$  representing the  $HH$  and  $VV$  coincidences that one may use as generators of a random output, and renormalize the matrix elements of the resulting  $2 \times 2$  subspace

density matrix  $\hat{\rho}_{\text{sub}}$  such that the diagonal elements add up to one [42].

For the CHSH-derived min-entropy bound [20–22], we consider the conditional min-entropy, denoted  $H_{\infty}(R|M)$ , which represents the min-entropy of the output  $R$  obtained after  $N$  measurements, given knowledge of the “input”  $M$ . Here this input  $M$  consists of the polarization measurement settings used for the photons in each measurement round. Pironio *et al.* [20] (see also Refs. [21,22] for improved proofs) showed that after  $N$  measurement rounds,  $H_{\infty}(R|M)$  is bounded from below by

$$H_{\infty}^{\text{min}}(R|M) = N \left[ 1 - \log_2 \left( 1 + \sqrt{2 - \frac{S^2}{4}} \right) \right] \quad \text{for } S \geq 2, \quad (2)$$

where  $S$  is the CHSH  $S$  value [36] estimated from the data collected in the  $N$  measurement rounds. Applied to the photonic scenario, the  $S$  value is defined as a linear combination of four expectation values:

$$S = E(\theta_{A1}, \theta_{B1}) + E(\theta_{A1}, \theta_{B2}) + E(\theta_{A2}, \theta_{B1}) - E(\theta_{A2}, \theta_{B2}), \quad (3)$$

where  $E(\theta_A, \theta_B) = \langle \hat{P}_{\theta_A, \theta_B} \rangle$ , and  $\hat{P}_{\theta_A, \theta_B} = \hat{P}_A(\theta_A) \otimes \hat{P}_B(\theta_B)$  denotes the observable representing a joint linear-polarization measurement on a pair of photons along the directions defined by the angles  $\theta_A$  and  $\theta_B$ . For the maximally entangled state  $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|H\rangle|H\rangle + |V\rangle|V\rangle)$ , the choices

$$\theta_{A1} = 0^\circ, \quad \theta_{A2} = 45^\circ, \quad \theta_{B1} = +22.5^\circ, \quad \theta_{B2} = -22.5^\circ \quad (4)$$

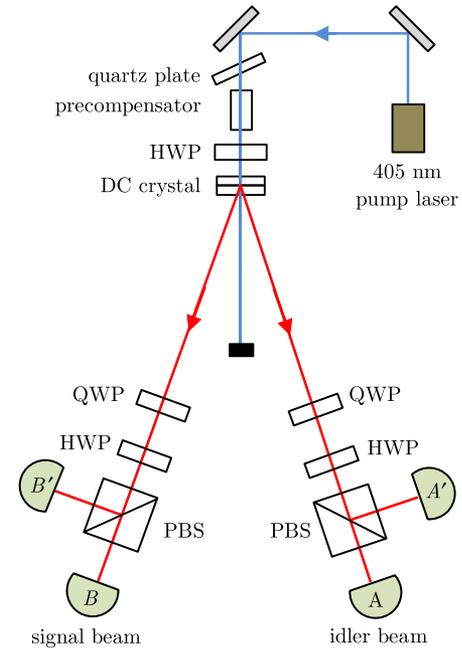
lead to the maximum possible value  $S = 2\sqrt{2}$ , while for any local realistic models, one has  $S \leq 2$  [5,36]. In the absence of superluminal signaling, CHSH-inequality violations show that the output cannot be entirely predetermined [7].

A rigorous experimental demonstration of CHSH-certified randomness would require closure of any Bell loopholes [5,23,44,45], which is beyond the scope of our experiment. In particular, the settings for each measurement would have to be chosen randomly. (In this sense, the CHSH-based randomness-certification protocol in Ref. [20] may be regarded as a randomness expander, since a small random seed used for the measurement settings is amplified into certifiable, private randomness through the measured CHSH violation [20,26].) Here our own aim is more modest: we use the measurement of the CHSH violation as an indicator of the presence of quantum randomness and of the nonclassical nature of the measured photon statistics.

### 3. EXPERIMENT

#### A. Experimental Setup

Our experimental setup is schematically shown in Fig. 1. A 405-nm, 150-mW diode laser pumps a pair of closely stacked, 0.5-mm-thick beta-barium borate crystals cut for type-I spontaneous parametric downconversion [46]. The optic axes of the crystals are oriented at right angles to each other, with one crystal producing pairs of horizontally polarized 810-nm photons, and the other crystal producing vertically polarized pairs.



**Fig. 1.** Schematic of the experimental setup. DC, downconversion crystal; HWP, half-wave plate; QWP, quarter-wave plate; PBS, polarizing beam splitter.  $A$ ,  $A'$ ,  $B$ , and  $B'$  represent assemblies containing converging lenses coupled to multimode fiber-optic cables that transmit photons to APD-based single-photon counting modules (not shown).

By equally pumping both crystals, we produce a polarization-entangled state resembling  $(|H\rangle|H\rangle + e^{i\phi}|V\rangle|V\rangle)/\sqrt{2}$ . We zero the phase  $\phi$  using an X-cut,  $10 \times 10 \times 0.5$  mm quartz plate to generate the Bell state  $|\Phi^+\rangle = (|H\rangle|H\rangle + |V\rangle|V\rangle)/\sqrt{2}$ . Entanglement quality is enhanced by a  $5 \times 5 \times 5.58$  mm quartz crystal that acts as a precompensator for the walk-off of the orthogonal polarization components inside the downconversion crystal. Signal and idler photons are measured by polarization analyzers composed of quarter-wave plates, half-wave plates, and polarizing beam splitters. Photons emerging from the outputs of the beam splitters are captured by converging lenses coupled to multimode fiber-optic cables and routed to single-photon counting modules based on silicon avalanche photodiodes with a detection efficiency of about 30% at 810 nm. Ambient photons are blocked by 780-nm long-pass filters mounted at the inputs of the photon counting modules. Photons in the signal and idler beams are measured in coincidence within a time window of about 7 ns. Coincidences are processed by a field-programmable gate array [47]. To quantify the closeness of the quantum state generated in our experiment to the Bell state  $\hat{\rho}_+ = |\Phi^+\rangle\langle\Phi^+|$ , we tomographically reconstruct the density matrix  $\hat{\rho}$  for the two-photon state. We calculate the fidelity  $F(\rho, \rho_+) = (\text{Tr}\sqrt{\sqrt{\rho}\rho_+\sqrt{\rho}})^2$  and find  $F(\rho, \rho_+) \approx 0.90$ .

#### B. Bit Generation

Our approach is to carry out a measurement of the violation of the CHSH inequality [5,36] as a verification of the presence of quantum randomness [20–23], and to use the same photon

counts produced from these polarization measurements to generate the bit sequence. In our experiment, we estimate the  $S$  value [see Eq. (3)] by measuring the four two-fold coincidence counts ( $AB$ ,  $A'B$ ,  $AB'$ , and  $A'B'$ ) at each of the four CHSH measurement settings  $(\theta_{A1}, \theta_{B1})$ ,  $(\theta_{A1}, \theta_{B2})$ ,  $(\theta_{A2}, \theta_{B1})$ , and  $(\theta_{A2}, \theta_{B2})$  given by Eq. (4). For each of these settings, we take  $5 \times 10^4$  samples, with each sample accumulated over a counting period of  $\tau = 0.2$  s. As our experiment does not aim to close loopholes associated with Bell tests [5,23,44,45], we do not employ random switching of the angles  $\theta_A$  and  $\theta_B$  between each sample. Instead, we take the full  $5 \times 10^4$  samples at a given angle setting and then change one of the angles to proceed to the next setting.

In this way, we obtain a total of  $2 \times 10^5$  samples (arising from the  $5 \times 10^4$  samples for each of the four angle settings), each containing four two-fold coincidence counts ( $AB$ ,  $A'B$ ,  $AB'$ , and  $A'B'$ ). We do not subtract accidental coincidences from the data. We calculate the CHSH  $S$  value given by Eq. (3) from the measured data and find  $S = 2.4618 \pm 0.0003$  (the error is estimated from count fluctuations between samples). We produce two different sequences from the measured coincidence count rates. A sequence  $\mathbf{x}_1$  containing  $2 \times 10^5$  bits is produced from the parity of the number  $N(AB)$  of  $AB$  coincidence counts in each of the  $2 \times 10^5$  samples. A sequence  $\mathbf{x}_2$  containing  $8 \times 10^5$  bits is produced by using, for each of the  $2 \times 10^5$  samples, the parity of each of the four coincidence counts  $N(AB)$ ,  $N(A'B)$ ,  $N(AB')$ , and  $N(A'B')$  to obtain a four-bit string per sample. While this gives a four-fold increase in the length of the sequence compared to  $\mathbf{x}_1$ , one may be concerned that the correlations inherent in the Bell state may introduce detectable correlations into the sequence. We will investigate this question below. Acquisition of the entire data set of  $2 \times 10^5$  samples (containing a total of about  $3 \times 10^8$  coincidence events) takes about  $10^3$  min, or about 16.7 h, and thus sequence  $\mathbf{x}_2$  is produced at a rate of 13.3 bits/s. [This is somewhat longer than the time one would expect based solely on the length of the counting interval, which is  $(2 \times 10^5 \text{ samples}) \times 0.2 \text{ s} = 4 \times 10^4 \text{ s} \approx 667$  mins. The reason for this discrepancy is that after each counting interval of 0.2 s is completed, there is a short lag of about 0.1 s before the next interval can be counted.]

## 4. RESULTS

### A. Min-Entropy Bounds

For the min-entropy bound obtained from quantum state tomography using Eq. (1), in Ref. [42], we report the results of the application of this equation to the quantum state prepared in our experiment, and here we shall simply restate these results. We find  $C = 0.44$  for the magnitude of the off-diagonal elements of the  $2 \times 2$  subspace density matrix  $\hat{\rho}_{\text{sub}}$  (where  $\hat{\rho}_{\text{sub}}$  is obtained from the two-photon density matrix in the manner described in Section 2). From Eq. (1), this gives  $H_{\infty}^{\text{min}} = 0.44$  per coincidence event.

For the min-entropy bound obtained from the CHSH violation via Eq. (2), our measured  $S$  value of  $S = 2.4618 \pm 0.0003$  implies a lower bound on the min-entropy of the output of approximately 0.24 per joint measurement (coincidence event). The fact that this bound is lower than the bound obtained from tomography may be understood by noting that the scope

of these two bounds is quite different. The CHSH-based bound (2) is nonzero only if the CHSH inequality is violated and thus the statistics cannot be modeled classically. In this way, its ultimate aim (in a loophole-free implementation) is the rigorous certification of private, secure randomness in a device-independent fashion [20–22]. The tomography-based bound (1), on the other hand, is nonzero whenever coherence between the two quantum states defining the relevant outcomes is present, and thus it *presumes* the quantum-mechanical tenet that such coherence gives rise to irreducible randomness [42].

### B. Randomness Testing

#### 1. Statistical Tests

We have subjected our generated bit sequences  $\mathbf{x}_1$  and  $\mathbf{x}_2$  to the statistical randomness tests provided by the NIST suite [33,48]. While such tests cannot positively identify the presence of randomness, they can flag sequences whose statistical patterns do not conform to the patterns expected for a uniform random process. For each NIST test applied to an input sequence, randomness is assessed in terms of a statistical quantity called the  $p$ -value. This is the probability that an ideal random number generator—such as a generator based on unbiased, independent coin tosses—would have produced a sequence less random (i.e., a sequence that performs worse in the test) than the sequence under inspection, given the type of nonrandom pattern searched for by the test [33]. For example, if a given test sequence scores a  $p$ -value of 0.01, then the chance that an ideal random source could have produced a sequence giving a lower (worse) result is one in 100. If  $p = 1$ , then the sequence is considered perfectly random with respect to the given test, while  $p = 0$  would indicate a completely nonrandom sequence.

Before running the tests, one sets the value of a confidence threshold parameter  $\alpha$ , and a given sequence is considered to pass the test if its  $p$ -value is no less than  $\alpha$ . We use the NIST default value  $\alpha = 0.01$  unless noted otherwise. First, we apply the tests to the entire sequences  $\mathbf{x}_1$  and  $\mathbf{x}_2$  to calculate their individual  $p$ -values. Of the 15 tests provided by the NIST suite, three tests (linear complexity, random excursions, and random excursions variant) cannot be applied because they require sequence lengths of at least  $10^6$  bits, and one other test (Maurer's) requires at least 387,840 bits and therefore can be applied only to sequence  $\mathbf{x}_2$ . Results are shown in Table 1. The  $p$ -values for all applicable tests are found to exceed the chosen confidence threshold  $\alpha = 0.01$ , and therefore the sequences can be considered random with a confidence of 99.9%.

To gather meaningful statistics in light of the chosen confidence threshold, one needs to subject at least  $1/\alpha$  sequences to each test, since even for an ideal random source, a fraction  $\alpha$  of sequences would be expected to fail the test, i.e., score  $p < \alpha$ . Therefore, next we let the NIST program break each sequence into  $N = 100$  nonoverlapping subsequences and run the tests on these subsequences. For three tests, our available sequence lengths impose constraints: (i) the binary matrix rank and Maurer's tests cannot be applied to subsequences of  $\mathbf{x}_1$  because of their insufficient length. (ii) For subsequences of  $\mathbf{x}_2$ , Maurer's test is likewise inapplicable; moreover, the minimum sequence lengths required for an application of the binary matrix rank and template matching tests dictate that we may decompose

**Table 1. Results of NIST Statistical Randomness Tests [33] Applied to the Sequences  $\mathbf{x}_1$  and  $\mathbf{x}_2$ <sup>a</sup>**

Statistical Test	Sequence $\mathbf{x}_1$			Sequence $\mathbf{x}_2$		
	<i>p</i> -Value	Proportion	<i>P</i> -Value	<i>p</i> -Value	Proportion	<i>P</i> -Value
Frequency	0.327383	100/100	0.153763	0.90035	99/100	0.071177
Frequency within a block	0.679802	100/100	0.437274	0.263874	100/100	0.045675
Runs	0.880981	100/100	0.455937	0.237737	98/100	0.595549
Longest run within a block	0.230194	100/100	0.153763	0.06073	98/100	0.759756
Cumulative sums (forward)	0.343646	100/100	0.924076	0.813301	99/100	0.137282
Cumulative sums (backward)	0.605296	100/100	0.275709	0.914125	99/100	0.062821
Discrete Fourier transform	0.189098	100/100	0.006196	0.651679	100/100	0.304126
Serial-1	0.510447	96/100	0.637119	0.55776	100/100	0.224821
Serial-2	0.161343	98/100	0.213309	0.318324	99/100	0.383827
Binary matrix rank	0.52999	n/a	n/a	0.134194	20/20	0.534146
Template matching	0.894736	18/20	0.534146	0.399080	97/100	0.040108
Approximate entropy	0.070835	98/100	0.334538	0.712837	100/100	0.595549
Maurer	n/a	n/a	n/a	0.650933	n/a	n/a

<sup>a</sup>Entries marked “n/a” indicate that a test could not be applied because of insufficient sequence length. The serial test produces two *p*-values as output, shown as “Serial-1” and “Serial-2.” For *p*-values, the following values for the block length parameter *m* are used: frequency within a block test,  $m = 2 \times 10^3$  for  $\mathbf{x}_1$  and  $m = 8 \times 10^3$  for  $\mathbf{x}_2$ ; serial test,  $m = 15$  for  $\mathbf{x}_1$  and  $m = 16$  for  $\mathbf{x}_2$ ; approximate entropy test,  $m = 10$ . For the “Proportion” values and *P*-values, the choices for *m* are: frequency within a block test,  $m = 20$  for  $\mathbf{x}_1$  and  $m = 80$  for  $\mathbf{x}_2$ ; serial test,  $m = 8$  for  $\mathbf{x}_1$  and  $m = 10$  for  $\mathbf{x}_2$ ; approximate entropy test,  $m = 5$  for  $\mathbf{x}_1$  and  $m = 7$  for  $\mathbf{x}_2$ . For the template matching applied to  $\mathbf{x}_1$  and the binary matrix rank applied to  $\mathbf{x}_2$ , a set of only 20 subsequences could be tested due to limited sequence lengths. The discrete Fourier transform test has been shown to have problems [49] that may render its reliability and sensitivity questionable.

$\mathbf{x}_2$  into only  $N = 20$  subsequences, implying a corresponding confidence threshold of only  $\alpha = 0.05$  (instead of  $\alpha = 0.01$ ). Test results are again given in Table 1. The column labeled “Proportion” lists the number of subsequences in the set that pass a test by scoring  $p \geq \alpha$ . The NIST suite considers the set of subsequences to pass the test if this proportion is larger than  $n_{\min} = 1 - \alpha - 3\sqrt{\alpha(1-\alpha)/N}$ , where  $N$  is the number of tested subsequences. For  $\alpha = 0.01$  and  $N = 100$ , this gives  $n_{\min} = 0.96$ , i.e., at least 96 out of 100 sequences must pass the test. For  $\alpha = 0.05$  and  $N = 20$ , we have  $n_{\min} = 0.80$ , i.e., the proportion must be at least 16/20. Our results show that the proportions of passing subsequences are all above these thresholds. The column labeled “*P*-value” in Table 1 represents the proximity of the distribution of *p*-values to a uniform distribution; passing a test corresponds to  $P \geq 0.0001$  [33]. All *P*-values are found to lie well above this threshold. In conclusion, our results show that the sequences  $\mathbf{x}_1$  and  $\mathbf{x}_2$  pass all applicable NIST tests.

## 2. Borel Normality

Since statistical tests such as those of the NIST suite were originally developed to test PRNGs, they are not necessarily sensitive to the particular issues and properties that characterize QRNGs. QRNGs that pass the NIST tests may struggle with tests that probe aspects of incomputability and algorithmic randomness, or show at least no marked advantage over PRNGs in terms of their algorithmic properties [28–30]. Here one particularly relevant and commonly used test is the Borel normality [24,34], which is a necessary (but not sufficient, e.g., Champernowne’s constant [50] is normal but computable) condition for algorithmic randomness and thus incomputability. It has been found to identify statistically significant differences between QRNGs and PRNGs, and the outputs of several experimental realizations of QRNGs have been shown not to be Borel normal [28–30]. The likely cause of the failure of Borel normality has

**Table 2. Results of the Borel-Normality Test**

Sequence	Bound <sup>a</sup>	$m = 1$	$m = 2$	$m = 3$	$m = 4$
$\mathbf{x}_1$	0.0094	0.0011	0.0014	0.0020	0.0024
$\mathbf{x}_2$	0.00495	0.00007	0.00090	0.00113	0.00109

<sup>a</sup>The bound is given by  $\sqrt{\log_2 |\mathbf{x}|/|\mathbf{x}|}$ , where  $|\mathbf{x}|$  is the sequence length, with  $|\mathbf{x}_1| = 2 \times 10^5$  and  $|\mathbf{x}_2| = 8 \times 10^5$ .

been attributed to experimental bias in the production of the bits [29,30].

Borel normality applied to a finite string measures whether all substrings of given length *m* occur with the expected probability of  $2^{-m}$  [24,34]. It relates to the compressibility of the string by a lossless finite-state machine [51]. A string  $\mathbf{x}$  of length  $|\mathbf{x}|$  is considered Borel normal if the following condition holds for all integers *m* with  $1 \leq m \leq \log_2 \log_2 |\mathbf{x}|$  [24,34]:

$$\max_{1 \leq j \leq 2^m} \left| \frac{N_j^m(\mathbf{x})}{|\mathbf{x}|/m} - \frac{1}{2^m} \right| \leq \sqrt{\frac{\log_2 |\mathbf{x}|}{|\mathbf{x}|}}, \quad (5)$$

where  $N_j^m(\mathbf{x})$  is the number of occurrences of the *j*th string drawn from the alphabet of all binary strings of length *m*. For our sequence lengths, the maximum value of *m* is  $m = 4$ . The results of the Borel-normality test applied to the two sequences  $\mathbf{x}_1$  and  $\mathbf{x}_2$  are shown in Table 2. The given values correspond to the left-hand side of Eq. (5) evaluated for  $\mathbf{x}_1$  and  $\mathbf{x}_2$ . Both sequences comfortably pass the test, as all values are well below the bound given by the right-hand side of Eq. (5). Note that for  $m = 1$ , the Borel-normality condition amounts to assessing the relative frequencies  $p_0$  and  $p_1$  of 0 s and 1 s. For our two sequences, this bias is extremely small: for  $\mathbf{x}_1$ , we have  $|p_0 - 0.5| = 1.1 \times 10^{-3}$ , and for  $\mathbf{x}_2$ , we have  $|p_0 - 0.5| = 7.0 \times 10^{-5}$ .

As an additional check, we also estimate the algorithmic complexity of the sequences  $\mathbf{x}_1$  and  $\mathbf{x}_2$  by calculating their

compressibility in terms of information density [52] using the program ENT [53]. We find information densities per bit of 0.998767 and 0.999739 for  $\mathbf{x}_1$  and  $\mathbf{x}_2$ , respectively. These values are very close to the maximum of one. This confirms that the sequences are virtually incompressible, indicating a large amount of randomness.

## 5. DISCUSSION

Our approach of using the parity of photon counts produces bias-free random numbers that pass the applicable statistical tests in the NIST suite and are Borel normal, without the need for an unbiasing postprocessing procedure or time-tagging. As we obtain the photon counts from a measurement of the CHSH violation for a polarization-entangled state, we can simultaneously confirm the nonclassical nature of the photon statistics and use the measured violation to estimate the min-entropy of the source. While a rigorous, loophole-free [23,45] demonstration of such certified randomness [20] is beyond the aim and scope of our experiment, the use of the measured CHSH violations may be regarded as a concurrent benchmark for assessing the randomness of the process and for complementing statistical and algorithmic tests of the output. The min-entropy bound we obtain from quantum state tomography serves as an additional confirmation of the presence of quantum randomness in the measured photon events. In this way, we may infer that the photon count statistics we measure are not just due to classical fluctuations, but are, at least in part, due to a genuinely quantum-mechanically random process without classical analog.

An obvious disadvantage of our method of generating bits from the parity of photon counts is its relative inefficiency, since we obtain just one number from a collection of photon events (namely, the number of counted photons in a given time interval  $\tau$ ) and extract only the least significant bit from that number. One effective way of substantially increasing the bit rate would be to make the counting interval  $\tau$  shorter. While the particular coincidence counting unit we use [47] does not allow for counting intervals shorter than  $\tau = 0.1$  s (limiting the bit rate to around 20 Hz), even relatively simple other units [48,54] provide the choice of much smaller intervals, and therefore the possibility of significantly higher bit rates. Another approach to boosting bit rates would be to use additional bits of the photon counts.

We note here that if time-tagging capabilities are available, one could alternatively apply the parity method for bit generation to the photon arrival times, rather than the photon counts, such that each photon event generates one bit. This was done, for example, in Ref. [29], where the resulting sequence was shown to be Borel normal. In such an experiment, however, a complementary verification of randomness via a min-entropy estimation from a CHSH violation or state tomography, as we have performed it, would not be possible in the same way, since the bits are not generated from measurements of polarization, which is the observable relevant to these types of min-entropy estimations.

Because the polarization-entangled state we generate implies the presence of correlations, the coincidence events  $AB$ ,  $A'B$ ,

$AB'$ , and  $A'B'$  are not independent, and one might be concerned that such correlations could diminish the randomness of the sequence  $\mathbf{x}_2$  produced from all four of these coincidences. This would indeed be the case if we were to generate each bit from individual measurement events rather than from parity, and a sequence experimentally produced in this way has been shown to fail the NIST tests [20]. The sequences  $\mathbf{x}_1$  and  $\mathbf{x}_2$ , however, both pass all of our randomness tests. Thus, within the scope of the tests we have performed, the Bell correlations do not have a detectable influence on the randomness of the sequence  $\mathbf{x}_2$ , indicating that the effect of such correlations becomes effectively washed out when considering the parity variable of accumulated counts.

**Funding.** M.J. Murdock Charitable Trust (NS-2015298); University of Portland (SURE-2019).

**Disclosures.** The authors declare no conflicts of interest.

## REFERENCES

1. B. Hayes, "Randomness as a resource," *Am. Sci.* **89**, 300–304 (2001).
2. R. Motwani and R. Rubinfeld, "Randomized algorithms," *ACM Comput. Surv.* **28**, 33–37 (1996).
3. N. Metropolis and S. Ulam, "The Monte Carlo method," *J. Am. Stat. Assoc.* **44**, 335–341 (1949).
4. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.* **74**, 145–195 (2002).
5. N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, "Bell nonlocality," *Rev. Mod. Phys.* **86**, 419–478 (2014).
6. M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum random number generators," *Rev. Mod. Phys.* **89**, 015004 (2017).
7. L. Masanes, A. Acin, and N. Gisin, "General properties of nonsignaling theories," *Phys. Rev. A* **73**, 012112 (2006).
8. T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, "A fast and compact quantum random number generator," *Rev. Sci. Instrum.* **71**, 1675–1680 (2000).
9. M. Fürst, H. Weier, S. Nauerth, D. G. Marangon, C. Kurtsiefer, and H. Weinfurter, "High speed optical quantum random number generation," *Opt. Express* **18**, 13029–13037 (2010).
10. M. Ren, E. Wu, Y. Liang, Y. Jian, G. Wu, and H. Zeng, "Quantum random-number generator based on a photon-number-resolving detector," *Phys. Rev. A* **83**, 023820 (2011).
11. J. F. Dynes, Z. L. Yuan, A. W. Sharpe, and A. J. Shields, "A high speed, postprocessing free, quantum random number generator," *Appl. Phys. Lett.* **93**, 031109 (2008).
12. M. Wahl, M. Leifgen, M. Berlin, T. Röhlicke, H.-J. Rahn, and O. Benson, "An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements," *Appl. Phys. Lett.* **98**, 171105 (2011).
13. C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauerer, U. L. Andersen, C. Marquardt, and G. Leuchs, "A generator for unique quantum random numbers based on vacuum states," *Nat. Photonics* **4**, 711–715 (2010).
14. Q. Zhang, X. Deng, C. Tian, and X. Su, "Quantum random number generator based on twin beams," *Opt. Lett.* **42**, 895–898 (2017).
15. Z. Zheng, Y.-C. Zhang, S. Yu, and H. Guo, "Experimental implementation of bias-free quantum random number generator based on vacuum fluctuation," in *7th International Conference on Photonics, Optics and Laser Technology* (SciTePress, 2019), pp. 276–282.
16. M. J. Collins, A. S. Clark, C. Xiong, E. Mägi, M. J. Steel, and B. J. Eggleton, "Random number generation from spontaneous Raman scattering," *Appl. Phys. Lett.* **107**, 141112 (2015).
17. M. Fiorentino, D. A. Fattal, C. M. Santori, S. M. Spillane, W. J. Munro, and R. G. Beausoleil, "Quantum information primitives using linear optics," *Proc. SPIE* **6305**, 63050E (2006).

18. M. Fiorentino, C. Santori, S. M. Spillane, R. G. Beausoleil, and W. J. Munro, "Secure self-calibrating quantum random-bit generator," *Phys. Rev. A* **75**, 032334 (2007).
19. T. Lunghi, J. B. Brask, C. C. W. Lim, Q. Lavigne, J. Bowles, A. Martin, H. Zbinden, and N. Brunner, "Self-testing quantum random number generator," *Phys. Rev. Lett.* **114**, 150501 (2015).
20. 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, and C. Monroe, "Random numbers certified by Bell's theorem," *Nature* **464**, 1021–1024 (2010).
21. S. Pironio and S. Massar, "Security of practical private randomness generation," *Phys. Rev. A* **87**, 012336 (2013).
22. S. Fehr, R. Gelles, and C. Schaffner, "Security and composability of randomness expansion from Bell inequalities," *Phys. Rev. A* **87**, 012335 (2013).
23. B. G. Christensen, K. T. McCusker, J. B. Altepeter, B. Calkins, T. Gerrits, A. E. Lita, A. Miller, L. K. Shalm, Y. Zhang, S. W. Nam, N. Brunner, C. C. W. Lim, N. Gisin, and P. G. Kwiat, "Detection-loophole-free test of quantum nonlocality, and applications," *Phys. Rev. Lett.* **111**, 130406 (2013).
24. C. Calude, *Information and Randomness: An Algorithmic Perspective*, 2nd ed. (Springer, 2010).
25. S. Kochen and E. Specker, "The problem of hidden variables in quantum mechanics," *J. Math. Mech.* **17**, 59–87 (1967).
26. A. A. Abbott, C. S. Calude, J. Conder, and K. Svozil, "Strong Kochen–Specker theorem and incomputability of quantum randomness," *Phys. Rev. A* **86**, 062109 (2012).
27. C. S. Calude and K. Svozil, "Quantum randomness and value indefiniteness," *Adv. Sci. Lett.* **1**, 165–168 (2008).
28. C. S. Calude, M. J. Dinneen, M. Dumitrescu, and K. Svozil, "Experimental evidence of quantum randomness incomputability," *Phys. Rev. A* **82**, 022102 (2010).
29. A. C. Martínez, A. Solís, R. D. H. Rojas, A. B. U'Ren, J. G. Hirsch, and I. P. Castillo, "Advanced statistical testing of quantum random number generators," *Entropy* **20**, 886–899 (2018).
30. A. A. Abbott, C. S. Calude, M. J. Dinneen, and N. Huang, "Experimentally probing the algorithmic randomness and incomputability of quantum randomness," *Phys. Scripta* **94**, 045103 (2019).
31. Y. Kang, H. X. Lu, Y. H. Lo, D. S. Bethune, and W. P. Risk, "Dark count probability and quantum efficiency of avalanche photodiodes for single-photon detection," *Appl. Phys. Lett.* **83**, 2955–2957 (2003).
32. D. B. Horoshko, V. N. Chizhevsky, and S. Y. Kilin, "Afterpulsing model based on the quasi-continuous distribution of deep levels in single-photon avalanche diodes," *J. Mod. Opt.* **64**, 191–195 (2017).
33. A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," NIST Special Publication 800-22, Revision 1a (National Institute of Standards and Technology, 2010).
34. C. S. Calude, "Borel normality and algorithmic randomness," in *Developments in Language Theory*, G. Rozenberg and A. Salomaa, eds. (World Scientific, 1994), pp. 113–129.
35. "quRNG," qutools, <https://www.qutools.com/qurng>.
36. J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, "Proposed experiment to test local hidden-variable theories," *Phys. Rev. Lett.* **23**, 880–884 (1969).
37. W. Wei and H. Guo, "Bias-free true random-number generator," *Opt. Lett.* **34**, 1876–1878 (2009).
38. M. Stipčević and J. E. Bowers, "Spatio-temporal optical random number generator," *Opt. Express* **23**, 11619–11631 (2015).
39. J. Wang, T. Xie, H. Zhang, D. Yang, C. Xie, and J. Wang, "A bias-free quantum random number generation using photon arrival time selectively," *IEEE Photon. J.* **7**, 1–8 (2015).
40. L. Nguyen, P. Rehain, Y. M. Sua, and Y.-P. Huang, "Programmable quantum random number generator without postprocessing," *Opt. Lett.* **43**, 631–634 (2018).
41. C. Cachin, *Entropy Measures and Unconditional Security in Cryptography*, ETH Series in Information Security and Cryptography (Hartung-Gorre, 1997).
42. M. R. Coleman, K. G. Ingalls, J. T. Kavulich, S. J. Kemmerly, N. C. Salinas, E. V. Ramirez, and M. Schlosshauer, "Assessing randomness with the aid of quantum state measurement," *Am. J. Phys.* **88**, 238–246 (2020).
43. B. Chor and O. Goldreich, "Unbiased bits from sources of weak randomness and probabilistic communication complexity," *SIAM J. Comput.* **17**, 230–261 (1988).
44. J. Åke Larsson, "Loopholes in Bell inequality tests of local realism," *J. Phys. A* **47**, 424003 (2014).
45. 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, K. J. Coakley, S. D. Dyer, C. Hodge, A. E. Lita, V. B. Verma, C. Lambrocco, E. Tortorici, A. L. Migdall, Y. Zhang, D. R. Kumor, W. H. Farr, F. Marsili, M. D. Shaw, J. A. Stern, C. Abellán, W. Amaya, V. Pruneri, T. Jennewein, M. W. Mitchell, P. G. Kwiat, J. C. Bienfang, R. P. Mirin, E. Knill, and S. W. Nam, "Strong loophole-free test of local realism," *Phys. Rev. Lett.* **115**, 250402 (2015).
46. P. G. Kwiat, E. Waks, A. G. White, I. Appelbaum, and P. H. Eberhard, "Ultrabright source of polarization-entangled photons," *Phys. Rev. A* **60**, R773–R776 (1999).
47. J. W. Lord and M. Beck, "Coincidence counting unit using the Altera DE2," <http://people.reed.edu/beckm/QM/circuit/circuit.html>.
48. D. Branning and M. Bermudez, "Testing quantum randomness in single-photon polarization measurements with the NIST test suite," *J. Opt. Soc. Am. B* **27**, 1594–1602 (2010).
49. H. Okada and K. Umeno, "Randomness evaluation with the discrete Fourier transform test based on exact analysis of the reference distribution," *IEEE Trans. Inf. Forensics Security* **12**, 1218–1226 (2017).
50. D. G. Champernowne, "The construction of decimals normal in the scale of ten," *J. London Math. Soc.* **s1-8**, 254–260 (1933).
51. J. Ziv and A. Lempel, "Compression of individual sequences via variable-rate coding," *IEEE Trans. Inform. Theory* **24**, 530–536 (1978).
52. R. W. Hamming, *Coding and Information Theory* (Prentice-Hall, 1980).
53. "ENT," <https://www.fourmilab.ch/random>.
54. D. Branning, S. Bhandari, and M. Beck, "Low-cost coincidence-counting electronics for undergraduate quantum optics," *Am. J. Phys.* **77**, 667–670 (2009).