Random number generation by coherent detection of quantum phase noise

Juan-Rafael Alvarez, S. Sarmiento, J. A. Lazaro, J. M. Gené, J. P. Torres

Optics EXPRESS

Random number generation by coherent detection of quantum phase noise

J.-R. Álvarez,[1,2,*] S. Sarmiento,[3] J. A. Lázaro,[3] J. M. Gené,[3] and J. P. Torres[1,3]

[1] ICFO - Institut de Cienciès Fotòniques, The Barcelona Institute of Science and Technology, 08860 Castelldefels, Barcelona, Spain
[2] University of Oxford, Clarendon Laboratory, Parks Road, Oxford OX1 3PU, UK
[3] Department of Signal Theory and Communications, Universitat Politècnica de Catalunya, 08034 Barcelona, Spain
[*] juan.alvarezvelasquez@physics.ox.ac.uk

Abstract: In 2010 Qi et al. [Opt. Lett. **35**(3), 312 (2010)] demonstrated a random number generator based on the drift of the phase of a laser due to spontaneous emission, The *out-of-the-lab* implementation of this scheme presents two main drawbacks: it requires a long and highly unbalanced interferometer to generate a random phase with uniform probability distribution, or alternatively, a shorter and slightly unbalanced interferometer that notwithstanding requires active stabilization and does not generate a uniform probability distribution without randomness extraction. Here we demonstrate that making use of the random nature of the phase difference between two independent laser sources and two coherent detectors we can overcome these limitations. The two main advantages of the system demonstrated are: i) it generates a probability distribution of quantum origin which is intrinsically uniform and thus in principle needs no randomness extraction for obtaining a uniform distribution, and ii) the phase is measured with telecom equipment routinely used for high capacity coherent optical communications. The speed of random bit generation is determined by the photodetector bandwidth and the linewidth of the lasers. As a by-product of our method, we have obtained images of how phase noise develops with time in a laser. This provides a highly visual alternative way of measuring the coherence time of a laser.

1. Introduction

Random numbers are routinely needed in many branches of science and technology. They are a key element in the development of secure communications channels, since random keys can provide unbreakable encryption systems [1]. They are used in banking, which uses the RSA algorithm that relies on the generation of random numbers [2]. They are important in gambling, where excellent random number generators are needed to guarantee the fairness of used machines. Governments are implementing technical standards on the usage of random number generators [3]. In scientific applications, Random Number Generators are behind powerful simulation methods such as Monte Carlo [4].

Random numbers are generated in many different ways. There are algorithms that generate streams of numbers (Pseudo-Random Number generators, PRNGs) that, in spite of not being truly random, can faithfully simulate true random sequences in many scenarios. There exist also methods which are based on deterministic processes, but for which our ignorance of the many variables involved make the possible outcomes random. This is the case of Random Number Generators (RNGs) based on the behavior of chaotic systems [5], certain geological events such as earthquakes, astronomical events, motion of computer mice, and interactions in social media [6–8].

#383196 https://doi.org/10.1364/OE.383196
Journal © 2020 Received 14 Nov 2019; revised 10 Jan 2020; accepted 15 Jan 2020; published 13 Feb 2020

Randomness sources based on the principles of quantum mechanics can provide true randomness which stems from fundamental physical phenomena [9]. In principle, the generated random keys are intrinsically random, as opposed to other random number generators based on different physical principles which might contain biases due to phenomena which are deterministic, yet unknown to an experimenter. Due to this, there is a lot of interest in the generation of random numbers based on the intrinsic and fundamental random character of quantum phenomena.

One particular phenomena that can be considered for Quantum Random Number Generation (QRNG) is the temporal drift of the phase of any laser source. Spontaneous emission of radiation, a quantum phenomena whose presence is inevitable in any lasing process, is responsible for such a phase drift. To be truly of quantum origin, we should use lasers where the drift of the phase comes from spontaneous emission and not from other sources of noise that can be termed as technical noise, changes in the conditions of the lasing operation. Phase noise based QRNGs, in combination with the use of pulsed lasers, have achieved speeds of the order of 43 Gbit/s [10]. These phase noise-based QRNGs have been a key element to close certain loopholes existing in Bell's inequalities tests [11].

In 2010, Qi *et al.* [12] demonstrated a phase noise based random number generator by passing the signal of a laser by an unbalanced Mach-Zehnder interferometer. The idea behind this experiment is interfering the laser signal at two different times so that the phase difference between these two signals is known to evolve randomly. The experimental setup for this situation is shown in Fig. 1(a).

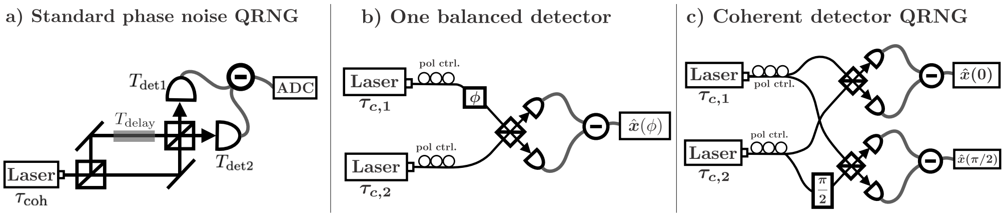


Fig. 1. (a) Depiction of an experimental setup for a phase noise interference Quantum Random Number generator, in which a laser interferes with itself at points where the phase has changed. (b) Schematic of a balanced detector, in which a phase ϕ is introduced in one of the lasers. A balanced detector with a phase delay ϕ can measure the quadrature $\hat{x}(\phi)$ of the interfering field. (c) Schematic of the setup used for a balanced coherent detector QRNG, which measures the quadratures of the interference between two lasers and thus obtains the phase noise of such interference.

If $\tau_{\rm coh}$ is the coherence time of the laser, $T_{\rm det}$ is the response time of the photodetectors, and $cT_{\rm delay}$ is the path difference between the two arms of the interferometer, two conditions should be fulfilled for Random Number Generation:

1. $T_{\rm delay} \gg \tau_{\rm coh}$ to guarantee that the phases of the signals traversing both arms of the interferometer are uncorrelated and the random phase difference obeys a uniform probability distribution.

2. $T_{\rm det} \ll \tau_{\rm coh}$ to ensure that we detect a fixed phase difference and we are not indeed integrating over a temporally-changing phase difference.

These conditions pose limitations on experimental realizations of this QRNG, as time delays of the order of τ_c imply very long path delays. Such delays are usually implemented using optical fiber cables. As an example, a coherence time of 0.01 milliseconds (a linewidth of 100 kHz), would require 3 additional kilometers of fiber in one of the arms of the interferometer.

The presence of long delays pose challenges due to the losses that fibres present, especially in non-telecom wavelengths, as well as their difficulty for possible integration in chips. One way to circumvent this drawback is using a slightly unbalanced interferometer that would generate a random phase with a non-uniform Gaussian-like probability distribution [12]. However, this calls for randomness extraction for obtaining a uniform probability distribution and the active stabilization of the interferometer that increases the technical difficulty of the implementation of the system.

Here we put forward and demonstrate a scheme where the quantum origin of the phase noise can be exploited for the generation of random number sequences without the need of using a highly unbalanced interferometer with long delays or phase stabilization in a slightly unbalanced interferometer. We use a second laser and measure the interference of the two laser sources with a pair of coherent detectors (for homodyne detection) that measure the phase variation directly. The method presented here builds up on works which have used the interference of two lasers to create RNGs [13–15], but the measurement of two orthogonal quadratures readily exposes the random behavior of the phase and requires a minimal amount of post-processing of the measured signal, since the probability distribution that obeys the random phase is uniform if samples are taken at intervals longer than the coherence time of the lasers.

Homodyne detection of optical signals is routinely done in optical communications laboratories with the help of optical hybrids. In optical communications, one is interested in extracting the real and imaginary part of a signal, which carries the information, with the help of a local oscillator that acts as reference signal. For random number generation, we are interested in extracting the phase difference between two signals.

In particular, we perform balanced coherent detection of two narrowband laser signals in the telecom band generated with external cavity lasers. By using fast sampling of the signal, of the order of ~ 100 Msamples/s, we are able to characterize the random walk performed by their phase difference, and determine their coherence times, i.e., the time over which the phases of the two lasers can be considered constant. When using slow sampling, of the order of ~ 100 kSamples/s, we are able to generate random numbers which do not require any sort of randomness extraction for obtaining a uniform probability distribution from a non-uniform one. We will show that without randomness extraction we can pass almost all of the standard statistical tests aimed at benchmarking RNGs. This is a feature that can be used for future, faster QRNGs, as we are able to provide true randomness with keys that are fast enough to feed randomness extractors with nonuniform distributions of quantum origin.

2. Theory

The source of randomness comes from the random phase difference between the signals coming from two different lasers. To measure such phases we make both signals to interfere with the help of balanced coherent detectors as shown in Figs. 1(b) and 1(c). These are optical arrangements which involve the use of phase delays and beam splitters. The signal of interest comes from the subtraction of the photocurrents measured by optical detectors at the two output ports of the beam splitter. The use of two balanced detectors with different phase delays makes it possible to recover the complex information of the interfering waves, in a configuration that is called a coherent detector. QRNGs using coherent detectors and the interference of the vacuum field with coherent fields have been described theoretically [16] and demonstrated experimentally [17].

Using a balanced detector with a phase delay ϕ, it is possible to measure the mean value of the quadrature $\hat{x}(\phi)$ of the interference between two lasers with frequencies $\omega_{1/2}$ and intensities $I_{1/2}$. This gives rise to a Skellam probability distribution for the measurement of the quadrature $\hat{x}(\phi)$ [16], which can be approximated as a normal probability distribution with mean $\sqrt{I_1 I_2}\cos(\Delta_\omega t + \phi)$ and variance $2(I_1 + I_2)$, where $\Delta_\omega = \omega_1 - \omega_2$.

As the phase changes in time due to spontaneous emission events occurring in the laser cavities, the signal measured by a balanced detector with a phase delay ϕ can be written as:

$$\langle x(\phi)\rangle \propto \sqrt{I_1 I_2}\cos\left(\Delta_\omega t + \xi(t) + \phi\right). \tag{1}$$

$\xi(t)$ is a normally distributed phase with zero mean and a variance that becomes broader as time progresses [14]:

$$\mathrm{var}\left(\xi(t)\right) = 2t\left(\frac{1}{\tau_{c,1}} + \frac{1}{\tau_{c,2}}\right) = \frac{t}{\overline{\tau}_c}, \tag{2}$$

where $\tau_{c,1/2}$ are the coherence times of the input lasers, defined as the inverse of their linewidths. Since $\xi(t)$ can only take values on the range $[-\pi, \pi]$, phases are wrapped around this range and are distributed according to a von Mises distribution [18]:

$$P\left(\xi(t) = \theta\right) = \frac{1}{2\pi I_0(t/\overline{\tau}_c)}\exp\left[\frac{\overline{\tau}_c}{t}\cos(\theta)\right]. \tag{3}$$

where $I_0(x)$ is the zeroth-order modified Bessel function of the first kind [19].

If the values of the phase are digitalized, the probability distribution of the phase can be made arbitrarily similar to a uniform distribution by measuring at times which are much longer than the coherence time. In other words, one can generate a uniform probability distribution for the random phase difference by decreasing the sampling rate at which the phase difference is measured. In particular, the measured values will follow a probability distribution of the form:

$$p_i = \int_{-\pi+i\delta}^{-\pi+i(\delta+1)} P\left(\xi(t) = \theta\right) d\theta \tag{4}$$

where $\delta = \frac{2\pi}{2^k}$, with k being the bit depth of the possible values in which θ can be discretized, and $i \in \left\{0, 2^k - 1\right\}$. With $t/\overline{\tau}_c > 2$ and $k = 8$, the maximum difference between p_i and u_i, the value of a uniform distribution, does not exceed 10^{-5}, i.e., it would take on average 10^5 values to observe a difference between the observed value and a uniform distribution, as shown in Fig. 2.

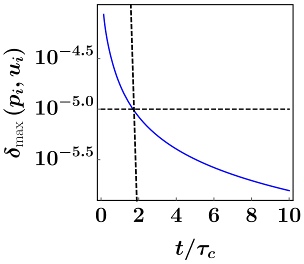


Fig. 2. Maximum difference between the discretized values of a von Mises distribution of variance t/τ_c and a uniform distribution. Here, the discretization is performed in 2^8 values.

3. Experimental setup and results

We performed experiments with two external cavity lasers (HP 8168A and Agilent 8164A) with central wavelengths around 1550nm, i.e., central frequencies around $\nu_0 \approx 193.4$THz. Central frequencies can typically vary 100 MHz per hour. In the experiments we measured typical central frequency differences between lasers of $\sim$ 1GHz, maintaining a stable beating interference for more than 20 hours. Both laser linewidths are approximately 100kHz, thus providing coherence times of $\tau_c \approx 20\mu s$. The laser powers are $P = 0.1\text{mW}$ at the photodetector end, corresponding to a mean photon flux numbers of $\Phi = (P/h\nu_0) \approx 7.8 \times 10^{14}$ photons/s.

Signals coming from the two lasers are sent to an optical hybrid (Kylia COH28) which provides the beam splitters and phase shifts that generate the two orthogonal quadrature readings of $\langle x(\phi)\rangle$ with $\phi = 0, \pi/2$. This optical hybrid reduces classical noise stemming from the fluctuation of the path lengths and phase shifters, being practically athermal, with phase variations of less than 17.5mrad for a change of ambient temperature of 90°C. Therefore we can safely neglect phase variations due to the interferometers during the time of detection [14].

The light exiting the optical hybrid is then fed to two balanced detectors (Thorlabs PDB480C-AC) with 1.6 GHz Bandwidth ($T_{\text{det}} = 625\text{ps}$). With this response time, detectors are able to measure $\approx 4.9 \times 10^5$photons per sample, generating a voltage with an amplitude of approximately 280 mV. In contrast, when no lasers are input, the electrical classical noise read by the detectors is normally distributed around 0 with a standard deviation of less than 7.5 mV. These values of signal and electrical noise are comparable in magnitude to those reported in [14]. With such values of photon numbers, high signal and low noise, it is possible to measure clean sinusoidal signals for the quadratures I and Q when they are sampled at rates on the order of GHz, as illustrated in Fig. 3(a). This is in contrast to experiments in which the vacuum field is one of the signals considered, in which case the shot noise is the determinant origin of randomness [16,17,20]. Finally, the readout is digitalized with an oscilloscope (Tektronix MSO 70804C) at sample rates ranging from 156.25kSamples/s to 25GSamples/s.

With measurements in two complementary quadratures, i.e. by measuring $I \equiv \langle x(0)\rangle$ and $Q \equiv \langle x(\pi/2)\rangle$, two signals whose amplitudes depend on the intensity fluctuations of both lasers, it is possible have access to the complete phase dynamics of $\xi(t)$ directly. I and Q follow probability distributions which are correlated and complementary. Having an additional quadrature provides additional information on the value of the phase in the unit circle instead of just one projection onto the axis, which has been the customary technique for developing phase noise QRNGs which utilize randomness extraction [10,14,21]. With this additional information, it is possible to retrieve a distribution which can be made arbitrarily similar to a Uniform distribution stemming from spontaneous emission. With the information provided by the signals I and Q and the unwrapping of the phase, we can reconstruct the phase behavior of the laser interference, compensating the classical drifts in intensity from both lasers:

$$\Theta(t) := \text{unwrap}(\arg(I + iQ)) = \Delta_\omega t + \xi(t)\,. \tag{5}$$

It is possible to eliminate the main, possibly classical frequency variation $\Delta_\omega t$, to obtain a phase variation which describes a random walk whose origin are the spontaneous emission kicks inside of the laser cavities. This is done by differentiating, subtracting the offset, and integrating again, i.e.:

$$\xi(t) = \int \left(\frac{d\Theta}{dt} - \Delta_\omega\right) dt. \tag{6}$$

The random values are obtained by further differentiating this phase ($d\xi/dt$), wrapping it to the range $]-\pi, \pi]$ and discretizing the possible outcomes to 8 bits. With this processing technique it is possible to recover the kicks in the phase distribution, following Eq. (3). The measurement of such phase distributions is shown in Fig. 4. With this technique in the measured experimental data, we are also able to recover directly the particular and different random trajectories of the phase.

As predicted by Eq. (3) and shown in Fig. 4, random phases start becoming uniformly distributed as time progresses. This can be seen on the histograms, which widen and flatten as the time between successive measurements becomes larger and thus converge to uniform distributions of uncorrelated data sets. The autocorrelation coefficient of a string of numbers Θ

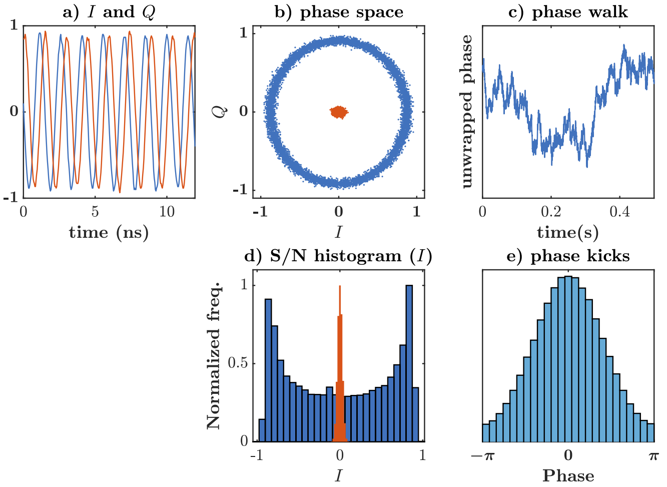


Fig. 3. Depiction of the processing methods used to measure the phase noise difference of the lasers. **(a)** is measured at sample rates of 25 GSamples/s, whereas **(b)**-**(e)** are measured at sample rates of 625 kSamples/s. **(a)** Presents an experimental measurement of the components I (dashed) and Q (continuous) as they are read out. It is noticeable that these two measurements are offset by $\pi/2$, and indeed they draw a circle when plotted against one another, as can be seen in **(b)**. **(b)** also shows a two-dimensional representation of the measured electrical noise, normalized to the maximum amplitude of the quadrature signals. Both I and Q are digitalized to 8 bits of depth, and are measured over several cycles, resulting in a thicker unit circle. A phase random walk is obtained by following the method of Eqs. 5 and 6. **(d)** Normalized histogram of measurements of the quadrature signal $I = \langle \hat{x}(0) \rangle$ after detection. Blue: arcsine distribution corresponding to the interference of the signals from the lasers. Orange: electrical noise, which corresponds to a narrow (typical deviation of 7.5 mV) normal distribution. The signal I and noise are normalized to the maximum value of the signal (285 mV). The standard deviation of the electrical noise accounts for less than 3 % of the measured signal amplitude. **(e)** Here we show the histogram of the different phase kicks that are recovered from the phase random walk in (c).

for a lag d [22], defined as

$$K_{\Theta\Theta}(d) = \frac{\sum_{i=1}^{N-d} (\Theta_i - \mathrm{mean}(\Theta)) (\Theta_{i+d} - \mathrm{mean}(\Theta))}{\mathrm{var}(\Theta)}, \tag{7}$$

never exceeds 2×10^{-3}, and the autocorrelation for up to 2.5×10^{6} samples is shown in Fig. 5. The autocorrelation for lag 0, which is by definition 1, is not shown. The measurement of this autocorrelation coefficients is shown as measured directly from the experiment, without any post-procesing apart from the one explained to retrieve the phase values. The autocorrelations with $d > 0$ are normally distributed with a mean zero and a standard deviation of 3.87×10^{-4}.

For random number generation, the measurements of I and Q are performed at 156.25 kSamples/s and digitalized at an 8-bit depth. Values of θ are saved as 8-bit values to reach a random number generator speed of 1.25MBits/s. We have tested the generation of uniform random numbers in a binary file of 21.21 Gbytes of data ($\approx 2^{37.3}$ bits), corresponding to 2.12×10^{10} measurements (as every measurement provides one byte) gathered in the experimental setup shown in Fig. 1(d). We have used three statistical suites generated for the verification of Random Number Generators: Robert G. Brown's dieharder [23], United States' National Institute of Standards and Technology (NIST)'s Statistical Testing Suite [24], and Pierre L'Ecuyer's TestU01's Alphabit testing battery, specifically designed for the testing of hardware Random

Optics EXPRESS

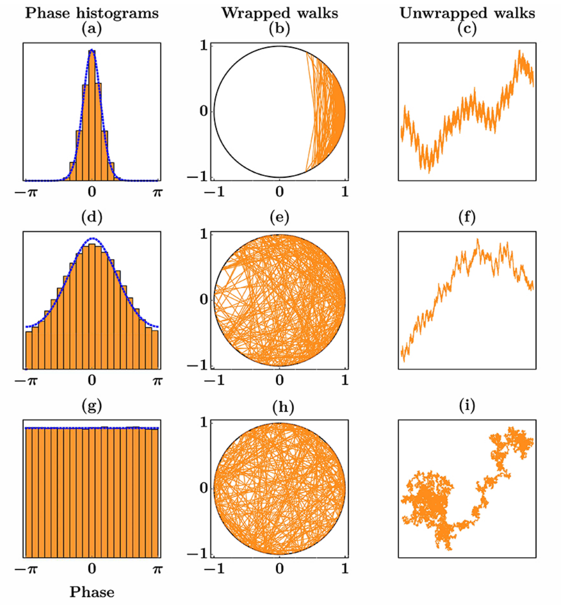


Fig. 4. Histograms (with corresponding fits) and phase space trajectories (wrapped in the phase space and unwrapped tail to tip) for three different sample rates, originating from 5 million point sample measurements on a balanced coherent detector sampled at **(a,b,c)** 7.81MSamples/s, **(d,e,f)** 500kSamples/s, and **(g,h,i)** 156.25kSamples/s. Only the first 300 points of each trajectory in the unit circle are shown, but 30 000 points are shown for the unwrapped walks. The loss of correlation between successive kicks starts to become noticeable once the sampling frequency is smaller than the laser linewidths, i.e., at about 200kHz. All histograms are fit with a von Mises distribution (Eq. (3)) with variance (a) $t/\overline{\tau_c} = 0.172$, (d) $t/\overline{\tau_c} = 1.78$, and (g) $t/\overline{\tau_c} = 7.50 \times 10^5$. (g) was additionally fit with a uniform distribution, with a Goodness of fit Kolmogorov-Smirnov test p-value of 0.56.

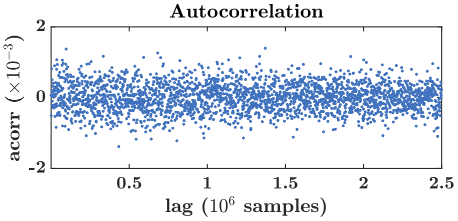
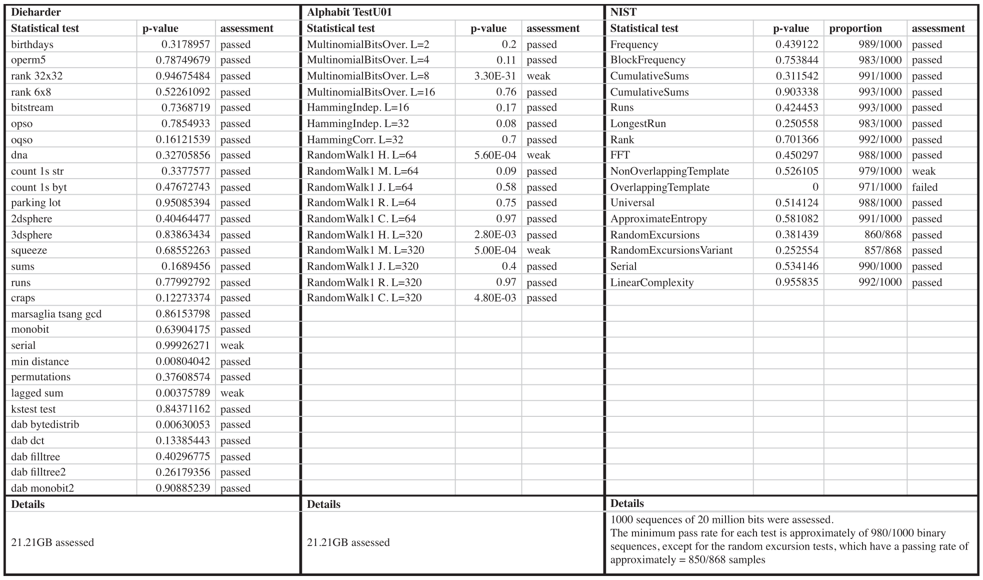


Fig. 5. Autocorrelation coefficients when the phase is being measured at rates of 156.25 kSamples/s.

Number Generators [25]. The random data sequence passes 304 out of the 311 random tests applied to it, in particular dieharder passing 115 of the 117 evaluated tests, NIST passing 175 of the 177 evaluated tests, and Alphabit passing 14 of the 17 evaluated tests. The results have been grouped under the smallest p-value.

The results of the dieharder statistical tests are presented in Table 1. A possible application for such a generator is the provision of true, quantum random data to feed the extraction of faster generators. Faster sources could be achieved by larger laser bandwidths, but this is a problem to be addressed in future work, as the wavelength stability of broader sources results in a loss of the beating which allows us to recover the phase noise.

Table 1. Statistical test results.



Dieharder			Alphabit TestU01			NIST			
Statistical test	**p-value**	**assessment**	**Statistical test**	**p-value**	**assessment**	**Statistical test**	**p-value**	**proportion**	**assessment**
birthdays	0.3178957	passed	MultinomialBitsOver. L=2	0.2	passed	Frequency	0.439122	989/1000	passed
operm5	0.78749679	passed	MultinomialBitsOver. L=4	0.11	passed	BlockFrequency	0.753844	983/1000	passed
rank 32x32	0.94675484	passed	MultinomialBitsOver. L=8	3.30E-31	weak	CumulativeSums	0.311542	991/1000	passed
rank 6x8	0.52261092	passed	MultinomialBitsOver. L=16	0.76	passed	CumulativeSums	0.903338	993/1000	passed
bitstream	0.7368719	passed	HammingIndep. L=16	0.17	passed	Runs	0.424453	993/1000	passed
opso	0.7854933	passed	HammingIndep. L=32	0.08	passed	LongestRun	0.250558	983/1000	passed
oqso	0.16121539	passed	HammingCorr. L=32	0.7	passed	Rank	0.701366	992/1000	passed
dna	0.32705856	passed	RandomWalk1 H. L=64	5.60E-04	weak	FFT	0.450297	988/1000	passed
count 1s str	0.3377577	passed	RandomWalk1 M. L=64	0.09	passed	NonOverlappingTemplate	0.526105	979/1000	weak
count 1s byt	0.47672743	passed	RandomWalk1 J. L=64	0.58	passed	OverlappingTemplate	0	971/1000	failed
parking lot	0.95085394	passed	RandomWalk1 R. L=64	0.75	passed	Universal	0.514124	988/1000	passed
2dsphere	0.40464477	passed	RandomWalk1 C. L=64	0.97	passed	ApproximateEntropy	0.581082	991/1000	passed
3dsphere	0.83863434	passed	RandomWalk1 H. L=320	2.80E-03	passed	RandomExcursions	0.381439	860/868	passed
squeeze	0.68552263	passed	RandomWalk1 M. L=320	5.00E-04	weak	RandomExcursionsVariant	0.252554	857/868	passed
sums	0.1689456	passed	RandomWalk1 J. L=320	0.4	passed	Serial	0.534146	990/1000	passed
runs	0.77992792	passed	RandomWalk1 R. L=320	0.97	passed	LinearComplexity	0.955835	992/1000	passed
craps	0.12273374	passed	RandomWalk1 C. L=320	4.80E-03	passed				
marsaglia tsang gcd	0.86153798	passed							
monobit	0.63904175	passed							
serial	0.99926271	weak							
min distance	0.00804042	passed							
permutations	0.37608574	passed							
lagged sum	0.00375789	weak							
kstest test	0.84371162	passed							
dab bytedistrib	0.00630053	passed							
dab dct	0.13385443	passed							
dab filltree	0.40296775	passed							
dab filltree2	0.26179356	passed							
dab monobit2	0.90885239	passed							
Details			**Details**			**Details**			
21.21GB assessed			21.21GB assessed			1000 sequences of 20 million bits were assessed. The minimum pass rate for each test is approximately of 980/1000 binary sequences, except for the random excursion tests, which have a passing rate of approximately = 850/868 samples			

4. Conclusions

We have demonstrated a quantum random number generator based on the extraction of the random phase difference between two laser beams. The simplicity of the processing techniques used and the availability and sturdiness of the components in telecom laboratories makes it easy to produce trusted random numbers for cryptographic purposes.

At slow speeds with high photon numbers, the phase noise is the dominant contribution to the random character of the interference of two lasers signals. The value of the phase is obtained by measuring two quadratures of the electric field of the two interfering lasers with a coherent detector. This randomness can be exploited to produce random numbers which do not require randomness extraction to obtain a uniform probability distribution from a non-uniform one, passing almost all of the standard statistical tests aimed at benchmarking Random Number Generators. We achieved a value of the autocorrelation coefficient of the random sequence of $\sim 4 \times 10^{-4}$. It thus provides a reliable source of true randomness that can be used for further calibration of faster randomness extractors.

The speed of random number generation can be further improved by measuring the randomness of the phase with broader sources, such as Distributed Feedback (DFB) lasers with a linewidth of 100MHz linewidth. Other RNGs using two lasers [14] consider CW lasers with coherence times of nearly $\overline{\tau}_c \sim 500$ ps, which corresponds to a bandwidth of some ~ 17 pm in wavelength. The theoretical limit for random number generation speed (without considering randomness extraction and sources of classical noise) is thus $\sim 1/\overline{\tau}_c = 2$ GHz. After randomness extraction and using a higher sampling rate to ensure a uniform probability distribution and a low value of the autocorrelation coefficient of the random sequence ($\sim 8 \times 10^{-3}$), a random number generation speed of 80 Mbit/s was achieved. In our particular case, although our generation speed only achieves approximately 1.25 Mbit/s, we could increase the RNG speed by decreasing the power of the laser, since it is well known that the bandwidth due to spontaneous emission is inversely proportional to the power generated in the lasing process [26,27]. However, this increase in speed might come at the expense of other considerations: the response time of photodetectors should be faster, and some sources of classical noise as photodetector noise might become relevant. Moreover, increasing the linewidths of the lasers and using more unstable sources might result in drifts of the laser beating.

The usage of narrowband sources such as the ones considered in this paper are a drawback to the speed of the key generation. However, it is important to remark that even though certain applications might require high-speed random number generation, in excess of a few Gbit/s, this is not a restrictive requisite in all possible applications. In important cases, the use of mature and easily accessible technology, the robustness or even the availability of the components needed for random number generation can be far more important considerations to take into account than the RNG speed [7]. In particular, the speed of the Random Number Generator here presented can be rapidly increased, but the laser sources used, although being very stable -thus allowing a beat note to be maintained over several hours-, are also narrow in linewidth, allowing for long coherence times. The lasers used are located on the regime where it is possible to observe how the phase distribution uniformizes.

Funding

Ministerio de Economía y Competitividad (FPI-BES-2015-074302 and TEC2017-90034-C2-2-R) supported by the European Regional Development Fund; H2020 Marie Skłodowska-Curie Actions (765075 (LIMQUET)).

Acknowledgments

JRA acknowledges V. Vicuña, M. Mitchell, M. Avesani, S. Zubieta, C. Leung, E. Kassa and A. Kuhn for useful discussions. JRA also thanks Fundació Catalunya-La Pedrera's ICFO Summer Fellows and the Europhotonics POESII Master. JPT acknowledges financial support from the Spanish Ministry of Economy and Competitiveness through the "Severo Ochoa" program for Centres of Excellence in R&D (SEV-2015-0522), from Fundació Privada Cellex, from Fundació Mir-Puig, and from Generalitat de Catalunya through the CERCA program.

Disclosures

The authors declare no conflicts of interest.

References

1. C. E. Shannon, "Communication theory of secrecy systems," Bell Syst. Tech. J. **28**(4), 656–715 (1949).
2. R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM **21**(2), 120–126 (1978).
3. M. S. Turan, E. Barker, J. Kelsey, K. A. McKay, M. L. Baish, and M. Boyle, "Recommendation for the entropy sources used for random bit generation," Tech. rep., NIST, (2018).
4. J. E. Gentle, *Random number generation and Monte Carlo methods*, Statistics and computing (Springer, 2003), 2nd ed.
5. L. L. Bonilla, M. Alvaro, and M. Carretero, "Chaos-based true random number generators," J. Math. Ind. **7**(1), 1 (2016).
6. C. Leung, A. Brown, H. Nguyen, A. S. Friedman, D. I. Kaiser, and J. Gallicchio, "Astronomical random numbers for quantum foundations experiments," Phys. Rev. A **97**(4), 042120 (2018).

7. S. Chen, "Random number generators go public," Science **360**(6396), 1383–1384 (2018).
8. Q. Zhou, X. Liao, K. wo Wong, Y. Hu, and D. Xiao, "True random number generator based on mouse movement and chaotic hash function," Inf. Sci. **179**(19), 3442–3450 (2009).
9. M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum random number generators," Rev. Mod. Phys. **89**(1), 015004 (2017).
10. C. Abellán, W. Amaya, M. Jofre, M. Curty, A. Acín, J. Capmany, V. Pruneri, and M. W. Mitchell, "Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode," Opt. Express **22**(2), 1645–1654 (2014).
11. M. Giustina, M. A. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J.-Å. Larsson, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, J. Beyer, T. Gerrits, A. E. Lita, L. K. Shalm, S. W. Nam, T. Scheidl, R. Ursin, B. Wittmann, and A. Zeilinger, "Significant-loophole-free test of bell's theorem with entangled photons," Phys. Rev. Lett. **115**(25), 250401 (2015).
12. B. Qi, Y.-M. Chi, H.-K. Lo, and L. Qian, "High-speed quantum random number generation by measuring phase noise of a single-mode laser," Opt. Lett. **35**(3), 312–314 (2010).
13. Q. Zhou, R. Valivarthi, C. John, and W. Tittel, "Practical quantum random-number generation based on sampling vacuum fluctuations," Quantum Eng. **1**(1), e8 (2019).
14. S.-H. Sun and F. Xu, "Experimental study of a quantum random-number generator based on two independent lasers," Phys. Rev. A **96**(6), 062314 (2017).
15. C. Abellan, W. Amaya, D. Domenech, P. Muñoz, J. Capmany, S. Longhi, M. W. Mitchell, and V. Pruneri, "Quantum entropy source on an InP photonic integrated circuit for random number generation," Optica **3**(9), 989–994 (2016).
16. H. Zhou, P. Zeng, M. Razavi, and X. Ma, "Randomness quantification of coherent detection," Phys. Rev. A **98**(4), 042321 (2018).
17. M. Avesani, D. G. Marangon, G. Vallone, and P. Villoresi, "Source-device-independent heterodyne-based quantum random number generator at 17 gbps," Nat. Commun. **9**(1), 5365 (2018).
18. K. V. Mardia and P. J. Zemroch, "Algorithm as 86: The von mises distribution function," J R Stat. Soc C.-Appl **24**(2), 268–272 (1975).
19. I. S. Milton Abramowitz, *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables* (Martino Fine Books, 2014).
20. 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**(10), 711–715 (2010).
21. M. W. Mitchell, C. Abellan, and W. Amaya, "Strong experimental guarantees in ultrafast quantum random number generation," Phys. Rev. A **91**(1), 012314 (2015).
22. K. I. Park, *Fundamentals of Probability and Stochastic Processes with Applications to Communications: Including a Concise Review of Mathematical Pre-requisites of Complex Variables, Matrix and Set Operations* (Springer Science+Business Media, 2017).
23. R. G. Brown, D. Eddelbuettel, and D. Bauer, "Dieharder: A Random Number Test Suite. Version 3.31.1,".
24. 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, N. A. Heckert, J. F. Dray, and S. Vo, "Sp 800-22 rev. 1a. a statistical test suite for random and pseudorandom number generators for cryptographic applications," Tech. rep., Gaithersburg, MD, United States, (2010).
25. P. L'Ecuyer and R. Simard, "Testu01: A c library for empirical testing of random number generators," ACM Trans. Math. Softw. **33**(4), 22–es (2007).
26. C. Henry, "Theory of the linewidth of semiconductor lasers," IEEE J. Quantum Electron. **18**(2), 259–264 (1982).
27. C. Henry, "Phase noise in semiconductor lasers," J. Lightwave Technol. **4**(3), 298–311 (1986).