Optical and Quantum Electronics (2023) 55:185
https://doi.org/10.1007/s11082-022-04396-y

Optical quantum random number generators: a comparative study

Omar Guillan-Lorenzo[1] · Marcos Troncoso-Costas[1,2] · David Alvarez-Outarelo[1] · Francisco Javier Diaz-Otero[1] · Juan Carlos Garcia-Escartin[3]

Received: 21 September 2022 / Accepted: 12 November 2022 / Published online: 4 January 2023

Abstract
Quantum random number generators give the opportunity to, in theory, obtain completely unpredictable numbers only perturbed by the noise in the measurement. The obtained data can be digitalized and processed so that it gives as a result a uniform sequence of binary random numbers without any relation with the classical noise in the system. In this work we analyze the performance of optical QRNGs with three different arrangements: a homodyne detector measuring vacuum fluctuations, a homodyne detector measuring amplified spontaneous emission from an EDFA and a spontaneous emission phase noise-based generator. The raw data from the experiments is processed using a Toeplitz extractor, giving as a result sequences of binary numbers capable of passing the NIST Statistical Test Suite.

Keywords Amplified spontaneous Emission · Quantum random number generator · Vacuum fluctuations

1 Introduction

It is apparent that information technologies and cryptography are the most demanding industries for random numbers, and therefore random number generation devices. There are however many other uses that heavily depend on random number generation, like the gambling industry or fundamental investigation.

Random number generators can be classified into three categories (Mannalath et al. 2022):

✉ Francisco Javier Diaz-Otero
fjdiaz@com.uvigo.es

Omar Guillan-Lorenzo
oguillan@com.uvigo.es

[1] atlanTTIC Research Center, EI Telecomunicacion, University of Vigo, Campus Universitario s/n, 36203 Vigo, Spain

[2] School of Electronic Engineering, Dublin City University, Glasnevin, Dublin 9 D09 V209, Ireland

[3] Dpto. Teoría de la Señal e Ing. Telemática, University of Valladolid, Paseo Belén 15, 47011 Valladolid, Spain

(1) Pseudorandom number generators (PRNG): seemingly random numbers are generated by means of an algorithm. The output sequence is hard to distinguish from a truly random one, but its order is totally predefined.

(2) True random number generators (TRNG):

  a. Physical random number generators: random numbers are generated upon measurements of classic systems parameters with chaotic behaviors; in special, chaos in lasers has been successfully used as a source of random bits at high frequencies (Kanter et al. 2010; Li et al. 2010; Li et al. 2018; Uchida et al. 2008). Output sequences are usually considered random, but at a fundamental level they are deterministic.
  b. Quantum random number generators (QRNG): random numbers are generated based on the uncertainty inherent to quantum physics (Gabriel et al. 2010).

In the last years, many experiments have been conducted relying on the quantum nature of light. In particular several authors have shown the operation of homodyne detectors in laboratory setups (Collett et al. 1987; Herrero-Collantes and Garcia-Escartin 2017) that can be extended to commercial use (Huang and Zhou 2019; Qi 2017; Raffaelli et al. 2018). There have also been shown major improvements obtained with the introduction of an Erbium-Doped Fiber Amplifier EDFA (Qi 2017). Those experiments used, nonetheless, different components, circuits and measurement equipment. In this paper we will present a thorough comparison of these methods, using a homogeneous setup for all of them. On top of that, we will conduct new experiments destined to analyze the influence of parameters such as laser power, EDFA pumping power or laser wavelength on a QRNG based on a homodyne receptor.

Classical monochromatic light waves have a quantum mechanical equivalence known as coherent states, which can be represented as a superposition of the photon number states. Unlike classical electromagnetic waves, phase and photon number of a coherent state have uncertainty in them and are always fluctuating around their average values.

The zero photon number state, more commonly known as the vacuum state, possesses a non-zero energy originated from a randomly fluctuating electromagnetic field (Glauber 1963) present even in the absence of photons. Measuring these random fluctuations will be one source of randomness in our experiments. The second source of randomness will rely on the phenomenon of amplified spontaneous emission (ASE) present in an EDFA, in which random noise from the spontaneous emission in the medium with population inversion is in turn amplified by stimulated emission in the medium. Lastly, we used as a source of randomness the phase noise resulting from spontaneous emission on two independent lasers operating at the same frequency.

2 Experimental setup

We present eight experiments based on the same laboratory setup, under the same conditions and with the same pieces of equipment (see Table 1), so the influence of laser wavelength or EDFA pumping power on QRNGs based on vacuum fluctuations or ASE as a randomness source can be compared and studied.

Table 1 Measured parameters in each experiment

Parameter #1	Parameter #2	Parameter #3	Experiment number
Laser 1.3 µm	Vacuum	Balanced fibers	3
	EDFA	10 mW	5
		13 mW	7
Laser 1.5 µm	Vacuum	Balanced fibers	1
		Unbalanced fibers	2
	EDFA	10 mW	4
		13 mW	6
Laser 1.5 µm + Laser 1.5 µm	Vacuum	Balanced fibers	8

The general homodyne detector setup consists of a 50:50 beam splitter, in which a laser is connected with a source of randomness (vacuum fluctuations/ASE). The outputs of the beam splitter are sent to two photoreceptors by optical fiber cables of the same length to avoid phase delays between the branches.

Both photodiodes must have similar characteristics so that the classical noise and oscillations from the laser get canceled out by taking the photocurrent difference which is proportional to the shot noise of the laser (Schumaker 1984; Yuen and Chan 1983).

The digitized difference of the photocurrents is recorded with an oscilloscope at a sampling frequency of 250 MS/s and 8 bits of resolution.

2.1 Vacuum fluctuations measurement

In experiments 1, 2, and 3 (Fig. 1a) the quantum noise was obtained by measuring the vacuum fluctuations in the electromagnetic field.

Experiments 1 and 3 used a laser source of 1549.32 and 1308.8 nm respectively.

Experiment 2 was designed to measure the effect of an unbalanced setup: one 1-meter fiber was used to connect the splitter to the first photodiode, while two 1-meter fibers were used in the connecting between the splitter and the second photodiode, thus changing the

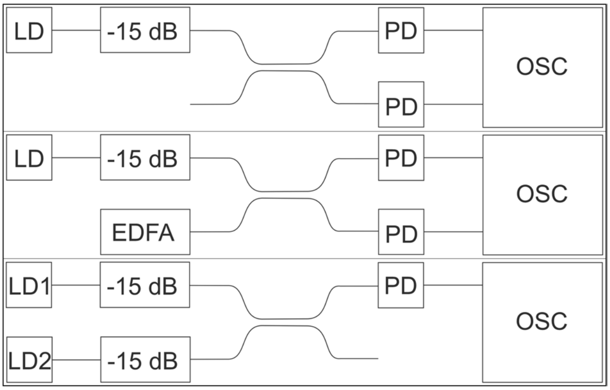


Fig. 1 Diagrams of laboratory setups for experiments 1–3 (top), 4–7 (middle) and 8 (bottom)

Table 2 Means and variances of measured Gaussian distributions

	Mean μ [V]	Variance σ² [V²]
Test 1	-2.71×10^{-4}	6.82×10^{-6}
Test 2	-2.61×10^{-4}	6.88×10^{-6}
Test 3	-2.67×10^{-4}	6.80×10^{-6}
Test 4	-2.50×10^{-4}	1.20×10^{-5}
Test 5	-2.38×10^{-4}	6.95×10^{-6}
Test 6	-2.32×10^{-4}	2.01×10^{-5}
Test 7	-2.39×10^{-4}	7.40×10^{-6}
Test 8 (non Gaussian)	3.43×10^{-1}	6.54×10^{-4}
Electronic noise 1	-2.42×10^{-4}	6.28×10^{-6}
Electronic noise 2	-2.30×10^{-4}	6.47×10^{-6}
Electronic noise 3	-2.42×10^{-4}	6.96×10^{-6}

length of the path that each light beam has to go through. The optical source was the same 1549.32 nm laser from experiment 1.

Laser sources, photodiodes, and beam splitter in the setup were the ones contained in the OptoSci ED-WDM kit.

2.2 ASE measurement

In experiments 4, 5, 6, and 7 (Fig. 1b) the setup is modified so ASE becomes the source of the quantum noise to be measured. That was accomplished by connecting an EDFA to the beam splitter input that was left open in experiments 1, 2, and 3. The used EDFA (from OptoSci ED-AMP kit) reaches saturation with a pumping power of 20 mW, so powers of 10 mW and 13 mW were selected in order to stay away from the upper limit.

Once again, two different laser wavelengths (1549.32 and 1308.8 nm) were alternatively connected to the first input of the beam splitter.

2.3 Vacuum fluctuations with channel multiplexing

In experiment 8 (Fig. 1c), two independent 1550 nm lasers were connected to the inputs of the beam splitter, thus producing a beat between the phase noise of both signals.

Table 3 Variance due to quantum noise and associated entropy

	$\sigma^2_{quantum}$ [V²]	H_∞ [bits per sample]
Test 1	5.41×10^{-7}	3.57
Test 2	6.01×10^{-7}	3.64
Test 3	5.26×10^{-7}	3.54
Test 4	5.51×10^{-6}	5.24
Test 5	4.75×10^{-7}	3.47
Test 6	1.31×10^{-5}	5.86
Test 7	4.41×10^{-7}	3.42
Test 8	2.98×10^{-6}	5.86

2.4 Electronic (non-quantum) noise measurement

Electronic noise measurements were performed by sampling the input signal in the oscilloscope while keeping the laser sources off. Four types can be distinguished:

(1) Electronic noise #1: tests without EDFA. Noise sources are photodiodes and the oscilloscope.
(2) Electronic noise #2: tests with EDFA at 10 mW pumping power. Noise sources are ASE, photodiodes, and the oscilloscope.
(3) Electronic noise #3: tests with EDFA at 13 mW pumping power. Noise sources are ASE, photodiodes, and the oscilloscope.
(4) Electronic noise #4: tests with a single laser to avoid noise beat. Noise sources are the photodiode, the oscilloscope, and the laser.

3 Measured data and postprocessing

3.1 Noise types and entropy

For each experiment, 5×10^5 samples of data have been recorded. The same number of samples have been taken for each of the four electronic noise types.

These sequences have been then undergone a normality test battery (Chi-square goodness of fit test, Lilliefors test, Kolmogorov-Smirnov test, and Jarque-Bera test) thus ensuring they fit a Gaussian distribution as predicted by theory (Glauber 1963) (except for experiment number 8).

The means and variances of the 11 Gaussian distributions are shown in Table 2:

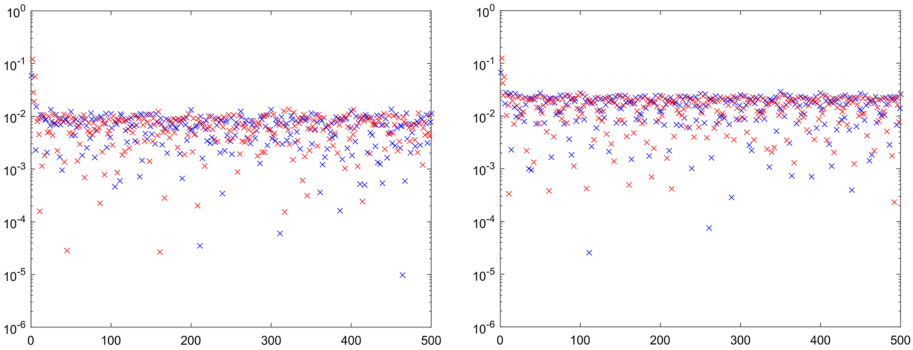


Fig. 2 autocorrelation coefficients from test 1 (left) and 2 (right). Positive values are in blue and negative values in red. (Color figure online)

Table 4 Length of the output sequence ($\epsilon = 2^{-50}$, $n = 5000$)

Test 1	Test 2	Test 3	Test 4	Test 5	Test 6	Test 7	Test 8
2132	2175	2113	3175	2069	3563	2038	2828

Fig. 3 : results of NIST Statistical Test Suite. Blue: values equal or over 0.01. Red: values under 0.01. ▶ **a** Test 1, sequence length 1.70 × 10^6; **b** Test 2, sequence length 1.74 × 10^6; **c** Test 3, sequence length 1.69 × 10^6; **d** Test 4, sequence length 2.54 × 10^6; **e** Test 5, sequence length 1.65 × 10^6; **f** Test 6, sequence length 2.85 × 10^6; **g** Test 7, sequence length 1.63 × 10^6; **h** Test 8, sequence length5.18 × 10^6 (Color figure online)

The signals recorded in each test are the combination of noises from quantum and non-quantum sources, being the latter unwanted because of not being purely non-deterministic.

Taking into account that both noises have different nature and origin, we can consider the quantum and the electronic noise to be independent (Sanguinetti et al. 2014; Ma et al. 2013), so the variance of the quantum noise can be calculated by subtracting the variance due to the electronic noise from the variance of the signal measured in the experiment (Table 3, second column).

For measuring and comparing the uncertainty of the sequences obtained in the different experiments, we calculated the min-entropy of experiments 1–7 as

$$H_{min} = \min_{1 \le i \le k}\left(-\log_2 p_i\right) = -\log_2\left(\max_{1 \le i \le k} p_i\right) \tag{1}$$

where $N = \{x1, x2, \ldots, x_k\}$ is the set of measurements with probabilities p_i for $i = 1, \ldots, k$ [12].

As the noise distribution in experiment 8 is not gaussian, an special analysis was required. The min-entropy was estimated by calculating the amount of bits that can be influenced by three standard deviations of the non-quantum noise associated to the experiment.

With an 8-bit digitalization of the raw data, the min-entropy calculation is shown in Table 3, third column:

It can be observed that entropy obtained in tests 4 and 6 is significantly higher than the others, thus demonstrating that min-entropy, and therefore, the random bits generation rate, increases with EDFA's pumping power.

Tests 5 and 7 yielded the lowest values for the min-entropy, thus showing that EDFA's improvement can only be leveraged by a laser with a wavelength within the amplification range.

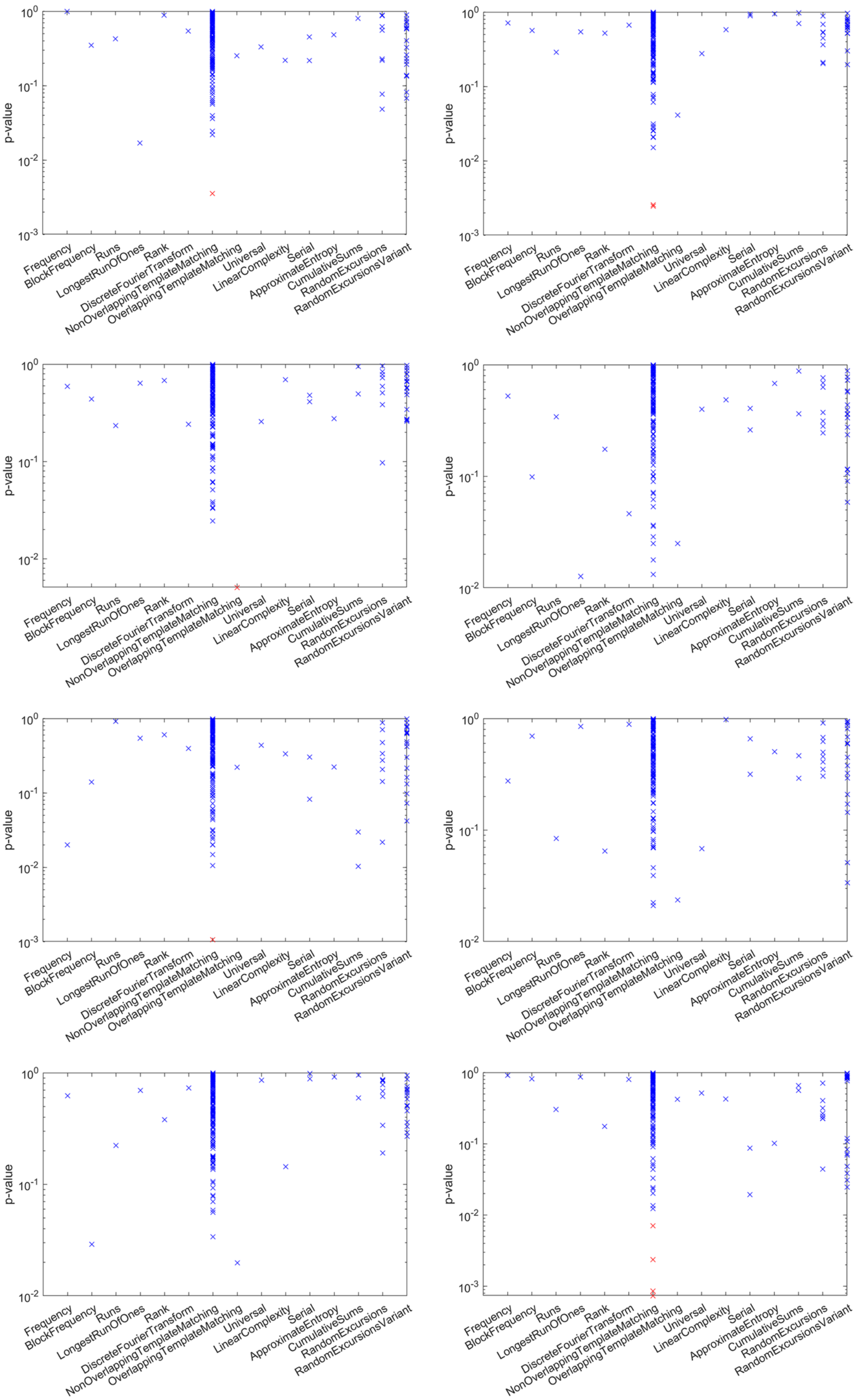
Entropy values from tests 1, 2 and 3 are very similar, which can lead us to think that neither wavelength nor fiber-optic links length make a difference. However, when comparing autocorrelation values for tests 1 and 2 (Fig. 2), a clear advantage of the balanced fibers setup over the unbalanced one is appreciated.

The two-laser setup from test 8 yields similar min-entropy values to those involving an EDFA.

3.2 Randomness extractors

The relatively low-entropy gaussian noise data obtained from the generator needs to be postprocessed with a randomness extractor, which will output a shorter, uniformly distributed sequence with higher entropy.

There are different techniques for this purpose, from which the Toeplitz matrix hashing has been chosen (Mansour et al. 1993; Krawczyk 1994) due to the high rate of generation it allows.


p-value
10^0
10^{-1}
10^{-2}
10^{-3}
Frequency
BlockFrequency
Runs
LongestRunOfOnes
Rank
DiscreteFourierTransform
NonOverlappingTemplateMatching
OverlappingTemplateMatching
Universal
LinearComplexity
Serial
ApproximateEntropy
CumulativeSums
RandomExcursions
RandomExcursionsVariant
p-value
10^0
10^{-1}
10^{-2}
10^{-3}
Frequency
BlockFrequency
Runs
LongestRunOfOnes
Rank
DiscreteFourierTransform
NonOverlappingTemplateMatching
OverlappingTemplateMatching
Universal
LinearComplexity
Serial
ApproximateEntropy
CumulativeSums
RandomExcursions
RandomExcursionsVariant
p-value
10^0
10^{-1}
10^{-2}
Frequency
BlockFrequency
Runs
LongestRunOfOnes
Rank
DiscreteFourierTransform
NonOverlappingTemplateMatching
OverlappingTemplateMatching
Universal
LinearComplexity
Serial
ApproximateEntropy
CumulativeSums
RandomExcursions
RandomExcursionsVariant
p-value
10^0
10^{-1}
10^{-2}
Frequency
BlockFrequency
Runs
LongestRunOfOnes
Rank
DiscreteFourierTransform
NonOverlappingTemplateMatching
OverlappingTemplateMatching
Universal
LinearComplexity
Serial
ApproximateEntropy
CumulativeSums
RandomExcursions
RandomExcursionsVariant
p-value
10^0
10^{-1}
10^{-2}
10^{-3}
Frequency
BlockFrequency
Runs
LongestRunOfOnes
Rank
DiscreteFourierTransform
NonOverlappingTemplateMatching
OverlappingTemplateMatching
Universal
LinearComplexity
Serial
ApproximateEntropy
CumulativeSums
RandomExcursions
RandomExcursionsVariant
p-value
10^0
10^{-1}
10^{-2}
Frequency
BlockFrequency
Runs
LongestRunOfOnes
Rank
DiscreteFourierTransform
NonOverlappingTemplateMatching
OverlappingTemplateMatching
Universal
LinearComplexity
Serial
ApproximateEntropy
CumulativeSums
RandomExcursions
RandomExcursionsVariant
p-value
10^0
10^{-1}
10^{-2}
Frequency
BlockFrequency
Runs
LongestRunOfOnes
Rank
DiscreteFourierTransform
NonOverlappingTemplateMatching
OverlappingTemplateMatching
Universal
LinearComplexity
Serial
ApproximateEntropy
CumulativeSums
RandomExcursions
RandomExcursionsVariant
p-value
10^0
10^{-1}
10^{-2}
10^{-3}
Frequency
BlockFrequency
Runs
LongestRunOfOnes
Rank
DiscreteFourierTransform
NonOverlappingTemplateMatching
OverlappingTemplateMatching
Universal
LinearComplexity
Serial
ApproximateEntropy
CumulativeSums
RandomExcursions
RandomExcursionsVariant

Let n be the length of the input sequence S, with min-entropy k. The length of the output sequence O can be calculated as $m = k + log_2\epsilon$, where ε is the security parameter, representing how close the distribution is from an ideal homogeneous one.

With this formula we computed for each experiment the length of the output sequence required for obtaining a security parameter of $\epsilon = 2^{-50}$ when setting an input length $n = 5000$. These results are shown in Table 4.

The output random sequence is finally generated according to the following procedure:

(1) We generated a sequence seed of $d = n + m - 1$ uniformly distributed pseudorandom numbers in the range $\{0,1\}$.
(2) From the previous sequence $\{a_i\}$, we built a Toeplitz matrix $T \in \mathcal{M}_{n\times m}/a_{ij} = a_{i+1,j+1}\ \forall a_{ij} \in T$.
(3) The output non-binary vector is calculated as $O' = S \times T$.
(4) Finally, a binarizing technique is applied so we get the final true random sequence $O = \left\{o_i\right\}$ where $o_i = o'_i \text{mod} 2$.

4 Randomness evaluation

Given a finite sequence of numbers, it is impossible to determine with absolute certainty whether they are random or not: a series of apparently random numbers may have a large repetition period so it is unnoticed and, conversely, a perfectly random sequence of numbers can show some repetitive patterns produced by chance.

Having that in mind, we decided to subject the outcome of our experiments to the NIST Statistical Test Suite (Bassham et al. 2010), consisting of a battery of 15 tests that compare different parameters of the sequence under study against the ones expected from a homogeneous random one. A test will be regarded as passed if the obtained p-value is over 0.01.

Our results (Fig. 3) show a high proportion of successful tests, with some values under 0.01 in experiments 1, 2, 3, 5 and 8. In spite of these under threshold values, since their proportion is very low, we can conclude with a high probability that the sequences are random and uniformly distributed.

5 Conclusion

It is possible to build a discrete quantum random number generator based on a homodyne detector.

The random number generation rate can be increased by using the ASE from and EDFA instead of solely the vacuum fluctuations.

Random bits generation rate increases with EDFA's pumping power while an imbalance in the length of the optical paths in the setup increases the autocorrelation coefficients of the measurements.

Finally, it is demonstrated that the use of two lasers provides better entropy values and higher random generation rates than setups relying on a single laser and vacuum fluctuations.

Author contributions All authors contributed to the study conception and design. Material preparation and data collection were performed by Marcos Troncoso-Costas and David Alvarez-Outerelo. Data processing

and analysis were performed by Marcos Troncoso-Costas, David Alvarez-Outerelo, Omar Guillan-Lorenzo, Francisco Javier Diaz-Otero and Juan Carlos Garcia-Escartin. Supervision and direction were performed by Francisco Javier Diaz-Otero. Expert advise on NIST and statistical procedures by Juan Carlos Garcia-Escartin. The first draft of the manuscript was written by Omar Guillan-Lorenzo and all authors commented on previous versions of the manuscript. All authors read and approved the final manuscript.

Funding Open Access funding provided thanks to the CRUE-CSIC agreement with Springer Nature. This project was supported by EU H2020 projects EDIFY (Contract Number 813467) and DRIVE-In (Contract Number 860763).

Data availability The datasets generated during and/or analysed during the current study are available from the corresponding author on reasonable request.

Declarations

Conflict of interest The authors have no relevant financial or non-financial interests to disclose.

Ethical approval Not applicable.

References

Bassham, L., et al.: A statistical test suite for random and pseudorandom number generators for cryptographic applications. (2010). https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=906762

Collett, M.J., Loudon, R., Gardiner, C.W.: Quantum theory of optical homodyne and heterodyne detection. J. Mod. Opt. **34**, 881–902 (1987)

Gabriel, C., et al.: A generator for unique quantum random numbers based on vacuum states. Nat. Photon. **4**, 711–715 (2010)

Glauber, R.J.: Coherent and incoherent states of the radiation field. Phys. Rev. **131**, 2766–2788 (1963)

Herrero-Collantes, M., Garcia-Escartin, J.C.: Quantum random number generators. Rev. Mod. Phys. **89**, 015004 (2017)

Huang, L., Zhou, H.: Integrated Gbps quantum random number generator with real-time extraction based on homodyne detection. J. Opt. Soc. Am. B. **36**, B130–B136 (2019)

Kanter, I., Aviad, Y., Reidler, I., Cohen, E., Rosenbluh, M.: An optical ultrafast random bit generator. Nat. Photon. **4**, 58–61 (2010)

Krawczyk, H.: LFSR-based hashing and authentication. In: Desmedt, Y.G. (ed.) Advances in cryptology–CRYPTO '94, pp. 129–139. Springer, Berlin (1994)

Li, P., Wang, Y.-C., Zhang, J.-Z.: All-optical fast random number generator. Opt. Express. **18**, 20360–20369 (2010)

Li, P., et al.: Ultrafast fully photonic random bit generator. J. Lightwave Technol. **36**, 2531–2540 (2018)

Ma, X.: Postprocessing for quantum random-number generators: entropy evaluation and randomness extraction. Phys. Rev. A **87**,(2013)

Mannalath, V., Mishra, S., Pathak, A.A.: Comprehensive review of quantum random number generators: concepts, classification and the origin of randomness. arXiv:2203.00261 (2022)

Mansour, Y., Nisan, N., Tiwari, P.: The computational complexity of universal hashing. Theor. Comput. Sci. **107**, 121–133 (1993)

Qi, B.: True randomness from an incoherent source. Rev. Sci. Instrum. **88**, 113101 (2017)

Raffaelli, F., et al.: A homodyne detector integrated onto a photonic chip for measuring quantum states and generating random numbers. Quantum Sci. Technol. **3**, 025003 (2018)

Sanguinetti, B., Martin, A., Zbinden, H., Gisin, N.: Quantum random number generation on a mobile phone. Phys. Rev. X. **4**, 031056 (2014)

Schumaker, B.L.: Noise in homodyne detection. Opt. Lett. **9**, 189–191 (1984)

Uchida, A., et al.: Fast physical random bit generation with chaotic semiconductor lasers. Nat. Photon. **2**, 728–732 (2008)

Yuen, H.P., Chan, V.W.: Noise in homodyne and heterodyne detection. Opt. Lett. **8**, 177–179 (1983)

Turan, M.S., et al.: Recommendation for the entropy sources used for random bit generation. NIST SP. 800–90b (2018). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800 https://doi.org/10.6028/NIST.SP.800-90B-90B.pdf

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.