OPTICS CONTINUUM

Quantum random number generator based on polarization switching in gain-switched VCSELs

MARCOS VALLE-MIÑÓN,[1] ANA QUIRCE,[1] ANGEL VALLE,[1,*] AND JAIME GUTIÉRREZ[2]

[1] *Instituto de Física de Cantabria (IFCA), Universidad de Cantabria-CSIC, Avda. Los Castros s/n, E39005, Santander, Spain*
[2] *Departamento de Matemática Aplicada y Ciencias de la Computación, Universidad de Cantabria, Avda. Los Castros s/n, E39005, Santander, Spain*
[*] *valle@ifca.unican.es*

Abstract: We experimentally study a quantum random number generator based on the random excitation of the linearly polarized modes of a gain-switched vertical-cavity surface-emitting laser (VCSEL). Our device is characterized by having polarization switching under continuous wave operation. By measuring the linear polarization mode that is excited in each pulse we collect a sufficient number of bits to evaluate if a standard statistical test suite is passed. We consider linear and Von Neumann post-processing methods in order to reduce the bias with different levels of bits rejection. The post-processed bit strings pass all tests in the standard test suite for random number generators provided by the National Institute of Standards and Technology (NIST). We finally compare the results obtained with different post-processing functions, including several $[n, k, d]$ linear BCH codes. We show that large values of n and k are the best choice to obtain simultaneously improved throughput and randomness.

1. Introduction

Random number generators (RNGs) are widely used in many applications including cryptographycally secured communications, industrial testing, Monte Carlo simulations, massive data processing, quantitative finance, etc. [1–3]. Quantum random number generators (QRNGs) stand out from RNGs because their randomness stems from quantum processes, this being the best guarantee for offering optimum privacy and security while maintaining high performance [2,3]. Using QRNGs is a necessary security requirement for quantum key distribution systems [4]. Most of the existing QRNGs are based on quantum optics. Single-photon [5–7] and multiphoton QRNGs [8–20] have been demonstrated. Quantum random number generation based on the phase fluctuations of the light emitted by a gain-switched edge-emitting semiconductor laser [14,15,18,20] is one of the most common multiphoton techniques. In these QRNGs, phase fluctuations are converted into amplitude fluctuations by using unbalanced Mach-Zehnder interferometry. Advantages of these type of generators include fast operation at Gbps rates, robustness, low cost, operation with flexible clock frequencies, and full integration on an InP platform [21], being also recently used for state preparation in quantum key distribution systems [4].

Very recently, QRNGs based on polarization switching (PS) in gain-switched vertical-cavity surface-emitting lasers (VCSELs) have been proposed [22–24]. This type of generators are also compact and fast, having the advantage of not requiring the interferometric element, essential in [14,15,18,20,21], from which the amplitude fluctuations and hence the random numbers are obtained. Also VCSELs offer advantages in comparison to edge-emitters, including compactness, high energy efficiency, low fabrication costs, on-wafer testing capability, and ease of 2D array packaging [25]. VCSELs show two orthogonal linearly polarized modes, and PS between them can be observed when changing the bias current [25,26]. The random nature of this PS is the

#464530 https://doi.org/10.1364/OPTCON.464530
Journal © 2022 Received 19 May 2022; revised 12 Aug 2022; accepted 7 Sep 2022; published 7 Oct 2022

basis of this QRNG as it has been theoretically proposed [22–24], and experimentally analyzed [24]. In this generator the current applied to a VCSEL is periodically changed from below the threshold current to a value well above threshold. The linear polarization that is preferably excited during the initial stages of pulse formation is random because it is determined by the sequence of spontaneous emission noise events. Random excitation of the VCSEL polarizations can be considered as a quantum entropy source because the amplified spontaneous emission is quantum mechanical in nature and can be considered as quantum noise [3,23,24,27,28].

It has been experimentally shown that for VCSELs having PS under continuous wave (cw) operation, similar probabilities of excitation of both linearly polarized modes can be achieved by adjusting the modulation conditions and the sampling time [24], opening the way for obtaining a low bias generator, that is with similar probabilities for "0" and "1" bits. However raw outputs of physical random number generators show deviations from the mathematical ideal of statistically independent and uniformly distributed bits [1,2,29–31], for instance in our case some bias can appear due to unwanted and slight variations of the experimental conditions. To address this problem an additional post-processing step is typically added to increase the bit entropy and to decrease bias in the raw bit stream. However this may come at the expense of throughput, for instance the Von Neumann processed bit stream is almost one quarter as long as the raw bit stream [30].

In the above mentioned experiment [24] the number of obtained random bits was not large enough in order to fully pass all tests in the standard test suite for random number generators provided by the National Institute of Standards and Technology (NIST) [32]. Our preliminar results indicated that statistical tests requiring small number of bits were passed. In this work we collect a much larger random bit stream in order to obtain significant statistical results. As mentioned above, post-processing of raw bit streams is necessary. We have considered different post-processing methods: the Von Neumann, as in [24], and a set of linear Bose–Chaudhuri–Hocquenghem (BCH) compression codes. We will use these linear compression techniques because it has been shown that they can achieve much better throughput than Von Neumann compression, while achieving practically good level of security [30].

Using these new sets of data we will show that the post-processed random bits obtained from our QRNG fully pass all the NIST tests. We will compare the results obtained with different post-processing methods in order to determine optimum performance in terms of throughput and statistical results in the NIST tests.

The paper is organized as follows. In Section 2 we describe the experimental setup, the method followed to obtain the random bits and the experimental results. Section 3 is devoted to describe the post-processing methods and the results of NIST tests. Finally, in Section 4 the discussion and conclusions are presented.

2. Experimental results

Our experimental all-fiber setup is shown in Fig. 1. A complete description of all their elements can be found in [24].

The VCSEL subject to gain-switching is a commercially available quantum-well long-wavelength (1550 nm) VCSEL (RayCan) with a threshold current, I_{th}= 2.51 mA at a temperature of 298 K. This temperature is maintained during all the measurements. Under cw operation PS is observed at a bias current of I_{PS} = 6.73 mA from the short-wavelength (labelled as y) to the long-wavelength (x) polarization mode [24]. The VCSEL is driven by the superposition of two electrical signals: a bias current (I_{off}, such that $I_{\mathrm{off}} < I_{\mathrm{th}}$) and a square signal provided by a pulse pattern generator. Both signals are superimposed by using a bias-tee as shown in Fig. 1. This signal is such that a voltage pulse of amplitude V_{on} is applied during half of the period, $T/2$, and no voltage is applied during the rest of the period. A polarization controller (PC) and a polarization beamsplitter (PBS) separate the two linear polarization modes of the VCSEL. These

OPTICS CONTINUUM

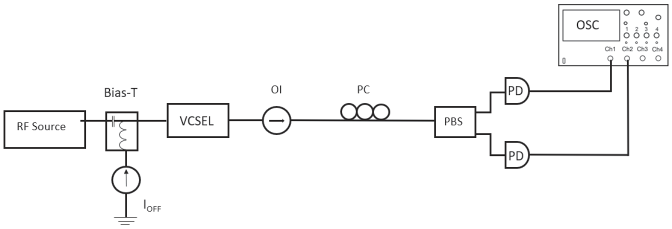

Fig. 1. Schematics of the experimental setup. OI: optical isolator, PC: polarization controller, PBS: polarization beam splitter, PD: photodetector, OSC: oscilloscope.

signals go to two fast photodiodes connected to a real-time oscilloscope (Keysight DSO91204A, with 13 GHz bandwidth).

Figure 2(a) shows the temporal waveforms of the $x-$ and $y-$signals measured at the oscilloscope, V_x and V_y, when the bias current is below threshold, I_{off}= 2.48 mA, T= 10 ns, and V_{on}=1.4 V, that corresponds to an applied current I_{on}=16 mA. These signals are proportional to the power of $x-$ and $y-$linearly polarized modes, respectively. The VCSEL switchs-off in all pulses in such a way that there is a random excitation of both linear polarizations after V_{on} is applied.

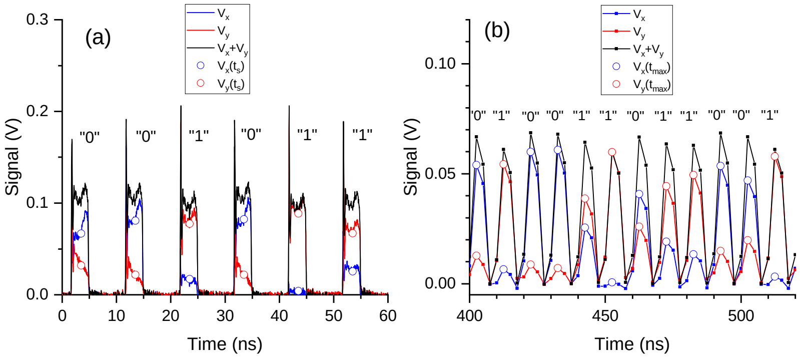

Fig. 2. Time traces of the signals corresponding to the x-polarization (blue line), y-polarization (red line), and total power (black line) for a sampling rate of (a) 40 GSa/s , and (b) 0.4 GSa/s. The signals at the sampling time, t_s = 3.5 ns, and the signals at the time of maximum total power are plotted with symbols in (a) and (b), respectively.

Polarization mode partition noise is also illustrated by plotting the signal corresponding to the total power: their fluctuations are much smaller than those corresponding to the individual polarizations. The random number generation process was performed in [24] in the following way, also illustrated in Fig. 2(a). A "0" ("1") bit was assigned when $V_x(t_s)$>$V_y(t_s)$ ($V_x(t_s) \leq V_y(t_s)$), where t_s is a chosen sampling time. Then, the probability of obtaining a "0" bit, $p(0)$, is the probability of excitation of the $x-$polarization at t_s, that is 0.52 for the conditions of Fig. 2(a) when considering 10^4 pulses. Figure 2(a) has been obtained with a sampling rate of 40 GSa/s at the oscilloscope working in the normal acquisition mode. This means that in each modulation period only one random bit is extracted from the 400 sampled values of the signals in each period.

To improve the efficiency for extracting the random bits we have acquired the data in the oscilloscope using the high resolution acquisition mode. In this acquisition mode the sampling rate is 40 GSa/s and two consecutive averages are performed in the oscilloscope. The first one is a boxcar average that considers high-resolution intervals of 80 points, and so for each period of the 100 MHz signal five values of the signal are obtained: S0· · · S4. These values are again averaged to obtain four high-resolution points in each period, HR0· · · HR3, in the following way: HR0=(S0+S1)/2,. . . 0, HR3=(S3+S4)/2. The results obtained are shown in Fig. 2(b). Four values of the signals are obtained each modulation period in such a way that a well defined maximum in the total power can be identified due to the low-pass filtering performed by this acquisition mode. We now obtain the random bits in a similar way than before but comparing V_x and V_y at the time at which the maximum of $V_x + V_y$ appears, t_{max}. Now, one random bit is obtained from the four values of the signals in each period. In this way a much larger number of random bits is obtained for a given number of recorded V_x and V_y. In our case 5.125×10^6 raw random bits are obtained from the 2.05×10^7 values of V_x and V_y that are recorded in each data file.

We show in Fig. 3(a) the values of $p(0)$ calculated for 788 bits sequences that we have obtained in temporal order. Each sequence has 5.125×10^6 bits, that are the raw bits obtained in each recorded data file. Initial values are close to 0.5, so the results are close to 0.52, that is the value obtained from the method used in [24] for extracting random bits. $p(0)$ fluctuates around 0.5 until the sequence #75 after which it suddenly increases to 0.61. A rather monotonous decrease is observed until sequence #170 after which $p(0)$ stabilizes again around 0.5. Figure 3(a) shows that the previous trend repeats another three times. The behavior shown in this figure can be explained by the way in which the measurements were performed. These were done in five sessions in such a way that all the equipment was switched off after each session. The beginning of the second, third, fourth and fifth sessions correspond to the numbers of the sequences at which the sudden increases are observed. This means that $p(0)$ stabilizes after a time of the order of 5 hours since the recording of each file takes around 4 minutes. Possibly this long stabilization time is due to a non optimum control of the temperature of the VCSEL in our setup.

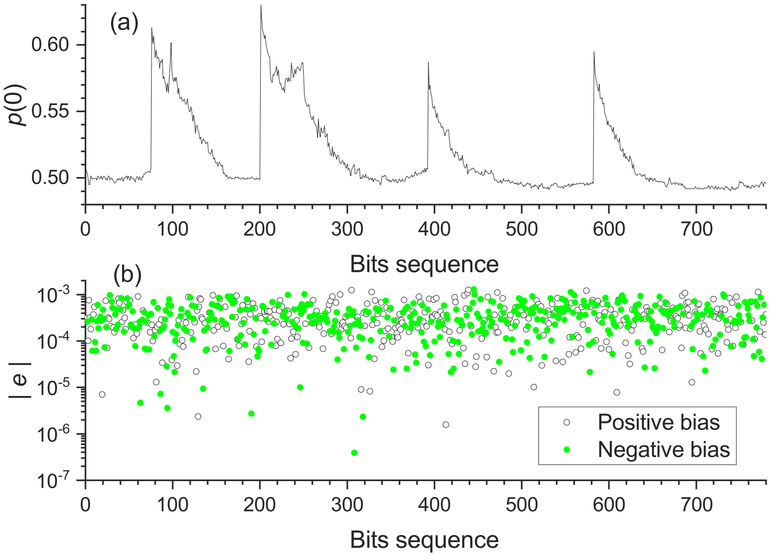

Fig. 3. (a) $p(0)$ obtained from the raw data bits, and (b) modulus of the bias obtained with the Von Neumann post-processing, for each of the bit sequences.

We now define the bias, e, of the random number generator by $e = p(0) - 1/2$. The value of the bias obtained for the complete set of raw bits of Fig. 3(a) (4.0385×10^9 bits) is $e = 1.54 \times 10^{-2}$. Since the value of the bias is large, post-processing of these raw bits is required in order to get random numbers that can pass the statistical tests. This will be the subject of the next section.

3. Post-processing methods and results of statistical tests

We first consider the non linear Von Neumann post-processing algorithm described in [1,30]. Von Neumann's is a very efficient method for reducing the bias with a modest throughput, that is the accepted bit rate is $0.25 - e^2$ [30]. We apply this algorithm to the complete set of raw bits shown in Fig. 3(a). In this way we obtain 788 sequences of 1.270487×10^6 post-processed bits each. We plot in Fig. 3(b) the absolute value of the bias for each of these sequences, distinguishing with colours the sign of the bias of each set. Post-processing largely decreases the bias values with respect to those corresponding to Fig. 3(a). The total number of post-processed bits is close to 10^9 for which $e = -3.1 \times 10^{-5}$.

We also consider the linear corrector codes post-processing techniques [31]. They are based on the following result:

Theorem 1 [31] *Let G be a linear corrector mapping n bits to k bits. Then the bias of any non zero linear combination of the output bits is less or equal than $2^{d-1}e^d$, where d is the minimal distance of the linear code constructed by the generator matrix G.*

As suggested in [30] we use the efficient $[n, k, d]$-BCH codes defined over the finite field $GF(2)$ and where $n + 1$ is a power of 2. For the raw input bits $(x_{n-1}, \ldots, x_0)$, the output $(y_{k-1}, \ldots, y_0)$ is obtained as:

$$\begin{pmatrix} g_{n-k} & \ldots\ldots\cdots . & g_0 & 0\cdots\ldots 0 \\ 0 & g_{n-k} & \cdots\ldots\ldots\cdots g_0 & 0\ldots\ldots 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0\ldots\ldots & 0 & g_{n-k} & \ldots\ldots g_0 \end{pmatrix} \begin{pmatrix} x_{n-1} \\ x_{n-2} \\ \vdots \\ x_0 \end{pmatrix} = \begin{pmatrix} y_{k-1} \\ y_{k-2} \\ \vdots \\ y_0 \end{pmatrix}$$

and $g(x) = g_{n-k}x^k + \cdots + g_1 x + g_0$ is the cyclic generator polynomial of the $[n, k, d]$-BCH code.

For instance the BCH code with parameters $[15, 7, 5]$ has as generator cyclic polynomial $x^8 + x^7 + x^6 + x^4 + 1$. Another example is the BCH code with parameters $[1023, 1003, 5]$ that has generator cyclic polynomial $x^{20} + x^{15} + x^{13} + x^{12} + x^{11} + x^9 + x^7 + x^6 + x^3 + x^2 + 1$ (see [33] for several properties of those practical linear codes).

The throughput, k/n, can be much larger than that obtained with Von Neumann's method, $\sim 1/4$, while maintaining a very efficient bias reduction $2^{d-1}e^d$ (see Theorem 1). This means that by choosing a k value slightly smaller than n a high throughput can be achieved.

Figure 4 shows the results obtained with the NIST statistical tests applied to the bits obtained with different post-processing techniques. Each test is performed using 1000 sequences of 1 million bits each with a statistical significance level, $\alpha = 0.01$. In Fig. 4 we show the P-value$_\mathrm{T}$, that gives an idea of the uniformity of the distribution of the P-values [32], and the proportion of sequences passing the tests for the Von Neumann and five different linear BCH codes. For tests that return multiple P-value$_\mathrm{T}$ and proportions, the more representative case, that is the one having a P-value$_\mathrm{T}$ closest to the median of P-value$_\mathrm{T}$, has been plotted. Two criteria are used in these tests for "success": i) the P-value$_\mathrm{T}$ must be larger than 10^{-4}, and ii) the proportions must be in the (0.9805607,0.9994393) confidence interval [32]. These values have been included in Fig. 4 using horizontal dashed lines. Results shown in Fig. 4 confirm that the post-processed bits sequences are sufficiently random for passing the statistical tests of NIST.

We now compare the performance of the different post-processing techniques. Table 1 shows the output bias, and the accepted bit rate for the post-processed data used in Fig. 4. We also include the P-value$_\mathrm{T}$ and the proportions averaged over the 16 tests, <P-value$_\mathrm{T}$> and <Prop>, in order to quantify in a summarised way the results of NIST tests. The spreading of proportions around <Prop> is also quantified by including the standard deviation of the proportions over the tests, σ_{Prop}.

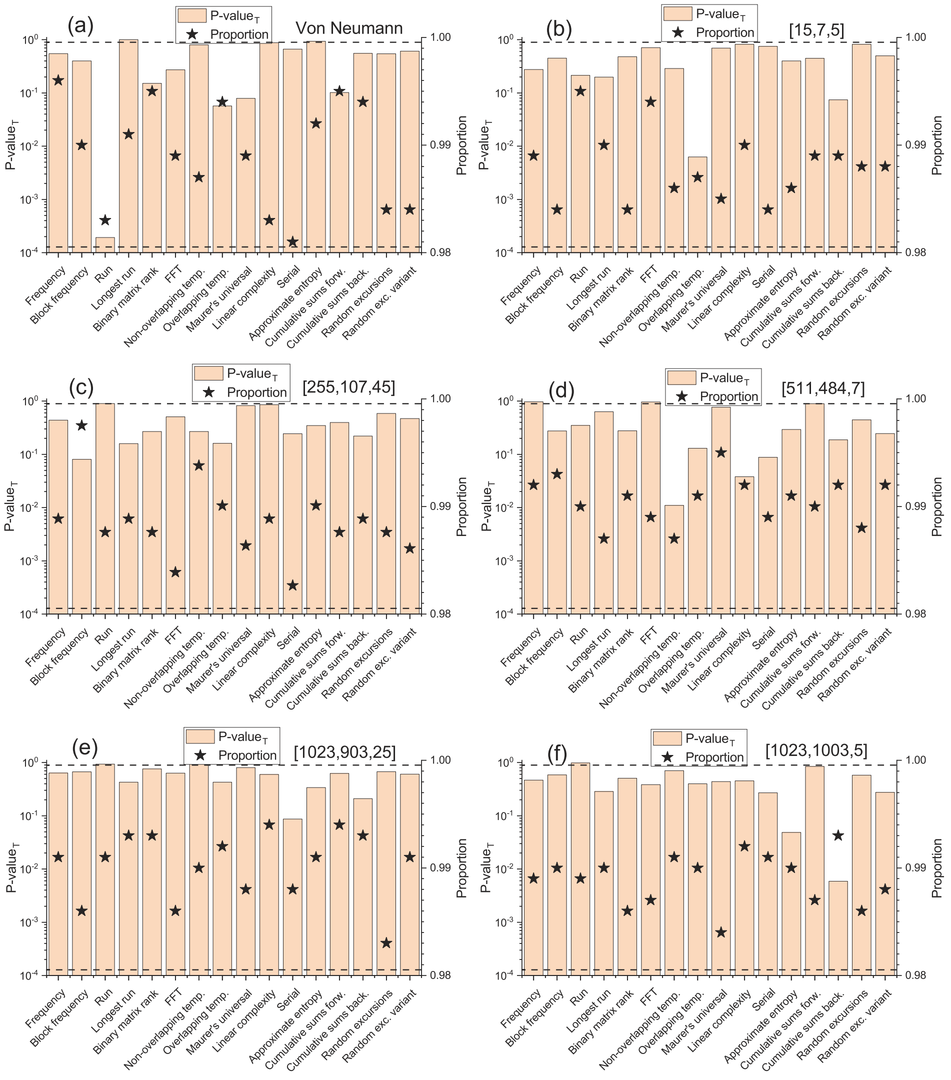

Fig. 4. NIST test results for data obtained using (a) Von Neumann, (b) [15,7,5], (c) [255,107,45], (d) [511,484,7], (e) [1023,903,25], and (f) [1023,1003,5] post-processing methods.

Table 1. Post-processing and NIST test results for different post-processing methods

Post-processing	Output bias	Rate	< P-value$_T$ >	< Prop >	σ_{Prop}
Von Neumann	-3.1×10^{-5}	0.2479	0.4737	0.9892	0.0050
[15,7,5]	-1.4×10^{-8}	0.4666	0.4446	0.9880	0.0033
[255,107,45]	-2.2×10^{-5}	0.4196	0.4204	0.9885	0.0035
[511,484,7]	8.2×10^{-6}	0.9472	0.4103	0.9906	0.0022
[1023,903,25]	9.0×10^{-6}	0.8827	0.5865	0.9903	0.0032
[1023,1003,5]	8.4×10^{-6}	0.9804	0.4513	0.9889	0.0024

Results on Table 1 show that all the post-processing methods are very efficient to reduce the bias, being the [15,7,5] method the one for which minimum | e | has been obtained. The accepted bit rate, given by the previously mentioned formulas, has a very wide range of variation, from the value close to 1/4 corresponding to Von Neumann's to the value 0.9804 obtained for [1023,1003,5]. The [1023,903,25] method, also with large values of n and k, gives the largest uniformity of the distributions of P-values because the obtained <P-value$_T$> is substantially larger than those found with the other methods, as it can be seen in Table 1 and in Fig. 4. Table 1 also shows that the averaged value of the proportions is always close to 0.99, as expected for a good RNG tested with $\alpha = 0.01$. The [511,484,7] and [1023,1003,5] methods have the smallest values of the standard deviation of the proportions. Results of Table 1 show that BCH codes with large values of n and k are the best choice to obtain simultaneously large values of throughput and <P-value$_T$> with a small standard deviation of the proportions around 0.99. The implementation in hardware of linear codes with large n and k utilizes more resources than those used with Von Neumann's method. However, Table 1 also shows that methods utilizing fewer resources than those with large values of n and k, like [15,7,5], permit to obtain similar <P-value$_T$> to those found with Von Neumann's but with a much larger throughput and smaller σ_{Prop}.

As mentioned in the previous section, the complete set of raw bits used for post-processing has a large bias value due to the way in which measurements were performed. A decrease of the large bias values observed in Fig. 3(a) could be obtained by measuring in just one long session after the bias stabilization is achieved. Alternatively, similar results can be expected if we select sequences of Fig. 3(a) in which $p(0)$ is close to 0.5. We have selected 200 sequences from the initial 788 sequences in which $p(0)$ is close to 0.5. We show in Fig. 5(a) the values of $p(0)$ for those selected sequencies of 5.125×10^6 raw bits each. The bias obtained with all the selected 1.025×10^9 raw bits is $e = -1.0 \times 10^{-4}$, much smaller than the $e = 1.54 \times 10^{-2}$ value obtained for all the raw bits.

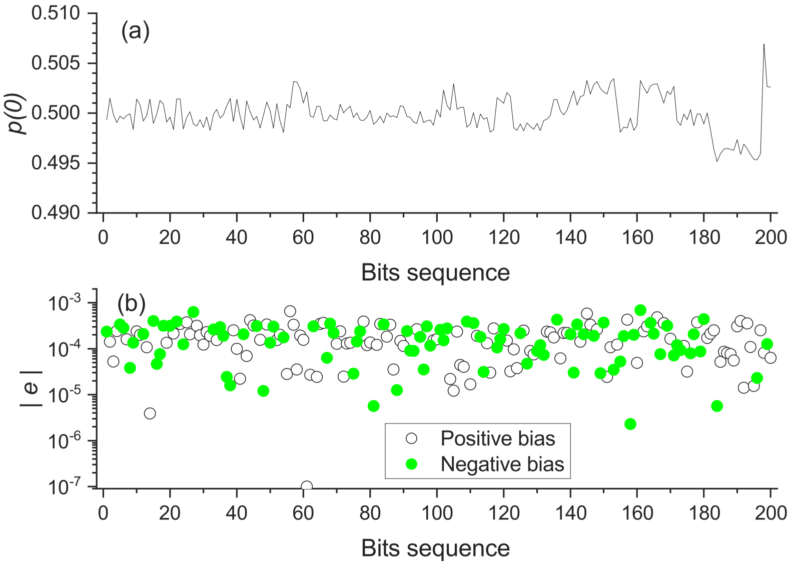

Fig. 5. (a) $p(0)$ obtained from the selected raw data bits, and (b) modulus of the bias obtained with the [1023,1003,5] post-processing, for each of the bit sequences.

We now wonder if this bias reduction is enough in order to pass the randomness tests with these selected raw data, so we have used them as input for the NIST statistical test suite with $\alpha = 0.01$. We have tested the randomness of 1024 sequences of 1 million bits each with the

NIST tests. There are eight tests for which the proportion of sequences that pass the tests is larger than 97.4% (longest runs, binary matrix rank, FFT, Maurer's universal, linear complexity, serial, random excursions and random excursions variant). The proportion obtained for the other eight tests does not reach the 97.4% value, going from 5.4% (run test) to 93.2% (approximate entropy test). In this way our selected raw data do not pass NIST tests. These results remark the necessity of a post-processing of the raw data in order to pass the complete set of NIST tests.

Our final step is to apply one of our post-processing methods to the set of selected raw bits. Then we apply the [1023,1003,5] method to the data set for which Fig. 5(a) was obtained. In this way we have 200 sequences of 5.0248×10^6 post-processed bits each. We plot in Fig. 5(b) the absolute value of the bias for each of these sequences. Post-processing largely decreases the bias values with respect to those shown in Fig. 5(a). The total number of post-processed bits is 1.00496×10^9 for which the bias is $e = 2.2 \times 10^{-5}$. From this set we take 1000 sequences of 10^6 post-processed bits as input of NIST tests. The results of NIST tests are shown in Fig. 6. The post-processed bits of the selected raw bit sequences are sufficiently random for passing the statistical tests of NIST. We can now compare these results with those obtained from post-processing the complete set of raw bits. Values of $<\text{P-value}_\text{T}>=0.5696$, $<\text{Prop}>=0.9879$, and $\sigma_\text{Prop} = 0.0038$ are obtained from Fig. 6. A comparison with results shown in Table 1 shows that the uniformity of the distribution of P-values significantly increases when using selected raw bits because $<\text{P-value}_\text{T}>$ has increased from 0.4513 to 0.5696. Also the smaller variation of bias obtained when using the selected set of raw bits results in the much larger value of P-value$_\text{T}$ for the Frequency test obtained in Fig. 6(a) (0.992) with respect to that found in Fig. 3(f) (0.467).

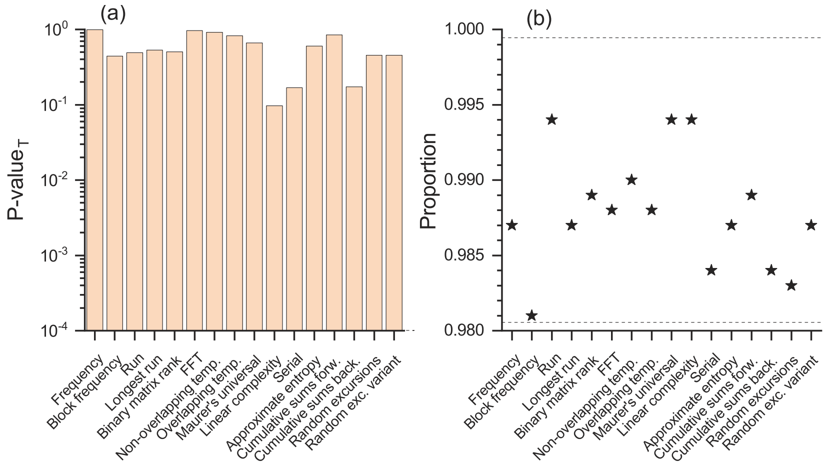

Fig. 6. NIST test results for the [1023,1003,5] post-processing of the selected raw data of Fig. 5. (a) P-value$_\text{T}$, and (b) proportions of sequencies that pass the tests

4. Discussion and conclusions

We have shown in the previous section that simple post-processings of the complete set of raw bits, characterized by large variations of the bias, have been enough in order to pass the NIST tests. This also means that our system for generating random bits would be practically unaffected by small variations in the modulation parameters provided that an appropriate post-processing is applied. The situation is similar when considering a better control of the experimental conditions because we have shown that post-processing of a subset of the previous raw data, characterized by a smaller variation of bias, also pass the NIST tests. This better control of the experimental conditions for obtaining low bias raw bits results in a significant improvement of the randomness of the post-processed data as shown by the large increase of the <P-value$_T$> that has been obtained in Fig. 6 with respect to that in Fig. 4(f).

In our experiment raw data bits have been generated at a rate of 100 Mbps. The bit rates that we have considered are not very fast but we want to remark that our main aim has been to collect a sufficient number of data to fully pass the NIST statistical tests. Taking into account that in [24] we demonstrated operation at twice the data rate of this work and that VCSEL's modulation bandwitdhs can go beyond 35 GHz [34] there is plenty of room to increase the generated random bit rate using our technique. Future work will be devoted to increase the gain-switching modulation rate, and hence to increase the random bit rate.

In this work we have considered different post-processing techniques, ranging from the non linear Von Neumann's to the family of linear BCH codes. These offer a large pool of codes to choose from in which it is possible to trade-off different aspects of a RNG performance, like output bias and throughput. BCH post-processing functions can be implemented in field-programmable gate array (FPGA) hardware circuitry [30]. FPGA implementations of BCH codes using the parity-check and the generator polynomials, with their corresponding resource utilization analysis, have been proposed and compared in [30]. Future work will also include the analysis using more classical post-processing methods, for example, the Trevisan extractor or the Toeplitz extractor.

Using a wide variety of compression codes our post-processed random bits have passed the NIST statistical tests. For tests that return multiple P-value$_T$ and proportions, the results corresponding to the worst case are sometimes found in the literature. We have considered instead the results that correspond to P-value$_T$ closest to the median of the P-value$_T$. We note that if we choose the worst case our results do not significantly change because all the tests are also passed and only a slight decrease of <P-value$_T$> with respect to that reported in Table 1 is observed. Some other randomness tests are frequently used, apart from NIST. We will also try to confirm the randomness of our data by using batteries of statistical tests like Dieharder, TestU01 and AIS 31. We also note that quantum randomness and classical noise must be considered to extract the real quantum noise. Future work will be devoted to propose models to ensure that the final randomness comes from quantum sources rather than classical ones.

Our setup uses complex controls mainly coming from the costly pulse pattern generator, and high bandwidth real-time oscilloscope. These elements can be substituted by devices reducing the cost, size and footprint of the equipment required for generating random numbers. The pulse pattern generator can be substituted by a step-recovery diode (SRD) in combination with a RF source. In fact, it has been recently shown that the use of an SRD as the electrical pulse generator gives similar results to those obtained with a pulse pattern generator in a system similar to that considered in our work [35]. The oscilloscope with the computer post-processing that we have used can be substituted by a comparator electronic circuit in combination with a FPGA implementation of the post-processing code. In fact, comparator hardware components are used in compact digitization systems for generating random numbers [36].

In conclusion we have shown that random bits obtained from polarization switching of linearly polarized modes in gain-switched VCSELs fully pass the batteries of the NIST SP800-22 statistical tests. We have compared the results obtained with different post-processing functions, including several $[n, k, d]$ linear BCH codes. We have shown that large values of n and k are the best choice to obtain simultaneously large values of throughput and <P-value$_T$>. These results indicate that our system is a good candidate for QRNG.

Funding. Ministerio de Ciencia e Innovación (PID2019-110633GB-I00MCIN/AEI/10.13039/501100011033, PID2021-123459OB-C22 MCIN/AEI/FEDER, UE).

Acknowledgments. A. Quirce acknowledges financial support from Beatriz Galindo program, Ministerio de Ciencia, Innovación y Universidades (Spain).

Disclosures. The authors declare no conflicts of interest.

Data availability. The data that support the plots within this letter and other findings of this study are available from the corresponding authors upon reasonable request.

References

1. M. Stipčević and Ç. K. Koç, "True random number generators," in *Open Problems in Mathematics and Computational Science*, (Springer, 2014), pp. 275–315.
2. M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum random number generators," Rev. Mod. Phys. **89**(1), 015004 (2017).
3. V. Mannalath, S. Mishra, and A. Pathak, "A comprehensive review of quantum random number generators: Concepts, classification and the origin of randomness," arXiv preprint arXiv:2203.00261 (2022).
4. T. K. Paraïso, R. I. Woodward, D. G. Marangon, V. Lovic, Z. Yuan, and A. J. Shields, "Advanced laser technology for quantum communications (tutorial review)," Adv. Quantum Technol. **4**(10), 2100062 (2021).
5. T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, "A fast and compact quantum random number generator," Rev. Sci. Instrum. **71**(4), 1675–1680 (2000).
6. W. Wei and H. Guo, "Bias-free true random-number generator," Opt. Lett. **34**(12), 1876–1878 (2009).
7. T. Durt, C. Belmonte, L.-P. Lamoureux, K. Panajotov, F. Van den Berghe, and H. Thienpont, "Fast quantum-optical random-number generators," Phys. Rev. A **87**(2), 022339 (2013).
8. H. Guo, W. Tang, Y. Liu, and W. Wei, "Truly random number generation based on measurement of phase noise of a laser," Phys. Rev. E **81**(5), 051137 (2010).
9. Y. Shen, L. Tian, and H. Zou, "Practical quantum random number generator based on measuring the shot noise of vacuum states," Phys. Rev. A **81**(6), 063814 (2010).
10. 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).
11. M. Jofre, M. Curty, F. Steinlechner, G. Anzolin, J. Torres, M. Mitchell, and V. Pruneri, "True random numbers from amplified quantum vacuum," Opt. Express **19**(21), 20665–20672 (2011).
12. A. Argyris, E. Pikasis, S. Deligiannidis, and D. Syvridis, "Sub-tb/s physical random bit generators based on direct detection of amplified spontaneous emission signals," J. Lightwave Technol. **30**(9), 1329–1334 (2012).
13. F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng, and H.-K. Lo, "Ultrafast quantum random number generation based on quantum phase fluctuations," Opt. Express **20**(11), 12366–12377 (2012).
14. C. Abellán, W. Amaya, M. Jofre, M. Curty, A. Acín, J. Capmany, V. Pruneri, and M. Mitchell, "Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode," Opt. Express **22**(2), 1645–1654 (2014).
15. Z. Yuan, M. Lucamarini, J. Dynes, B. Fröhlich, A. Plews, and A. Shields, "Robust random number generation using steady-state emission of gain-switched laser diodes," Appl. Phys. Lett. **104**(26), 261112 (2014).
16. D. G. Marangon, A. Plews, M. Lucamarini, J. F. Dynes, A. W. Sharpe, Z. Yuan, and A. J. Shields, "Long-term test of a fast and compact quantum random number generator," J. Lightwave Technol. **36**(17), 3778–3784 (2018).
17. B. Septriani, O. de Vries, F. Steinlechner, and M. Gräfe, "Parametric study of the phase diffusion process in a gain-switched semiconductor laser for randomness assessment in quantum random number generator," AIP Adv. **10**(5), 055022 (2020).
18. R. Shakhovoy, D. Sych, V. Sharoglazova, A. Udaltsov, A. Fedorov, and Y. Kurochkin, "Quantum noise extraction from the interference of laser pulses in an optical quantum random number generator," Opt. Express **28**(5), 6209–6224 (2020).
19. R. Shakhovoy, V. Sharoglazova, A. Udaltsov, A. Duplinskiy, V. Kurochkin, and Y. Kurochkin, "Influence of chirp, jitter, and relaxation oscillations on probabilistic properties of laser pulse interference," IEEE J. Quantum Electron. **57**(2), 1–7 (2021).
20. V. Lovic, D. G. Marangon, M. Lucamarini, Z. Yuan, and A. J. Shields, "Characterizing phase noise in a gain-switched laser diode for quantum random-number generation," Phys. Rev. Appl. **16**(5), 054012 (2021).
21. C. Abellan, W. Amaya, D. Domenech, P. Mu noz, 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).
22. J. Zhao, P. Li, X. Zhang, Z. Gao, Z. Jia, A. Bogris, K. A. Shore, and Y. Wang, "Fast all-optical random number generator," arXiv preprint arXiv:2201.07616 (2022).
23. R. Shakhovoy, E. Maksimova, V. Sharoglazova, M. Puplauskis, and Y. Kurochkin, "Fast and compact vcsel-based quantum random number generator," J. Phys.: Conf. Ser. **1984**(1), 012005 (2021).
24. A. Quirce and A. Valle, "Random polarization switching in gain-switched vcsels for quantum random number generation," Opt. Express **30**(7), 10513–10527 (2022).
25. R. Michalzik, *VCSELs: fundamentals, technology and applications of vertical-cavity surface-emitting lasers*, vol. 166 (Springer, 2012).
26. K. D. Choquette, R. P. Schneider, K. L. Lear, and R. E. Leibenguth, "Gain-dependent polarization properties of vertical-cavity lasers," IEEE J. Sel. Top. Quantum Electron. **1**(2), 661–666 (1995).
27. R. Loudon, *The quantum theory of light* (OUP Oxford, 2000).
28. L. A. Coldren, S. W. Corzine, and M. L. Mashanovitch, *Diode lasers and photonic integrated circuits*, vol. 218 (John Wiley & Sons, 2012).

OPTICS CONTINUUM

29. M. Dichtl, "Bad and good ways of post-processing biased physical random numbers," in *International Workshop on Fast Software Encryption*, (Springer, 2007), pp. 137–152.
30. S.-H. Kwok, Y.-L. Ee, G. Chew, K. Zheng, K. Khoo, and C.-H. Tan, "A comparison of post-processing techniques for biased random number generators," in *IFIP International Workshop on Information Security Theory and Practices*, (Springer, 2011), pp. 175–190.
31. P. Lacharme, "Post-processing functions for a biased physical random number generator," in *International Workshop on Fast Software Encryption*, (Springer, 2008), pp. 334–342.
32. 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, "NIST special publication 800-22: a statistical test suite for the validation of random number generators and pseudo random number generators for cryptographic applications," NIST Special Publication **800**, 22 (2010).
33. F. J. MacWilliams and N. J. A. Sloane, *The theory of error correcting codes*, vol. 16 (Elsevier, 1977).
34. A. Liu, P. Wolf, J. A. Lott, and D. Bimberg, "Vertical-cavity surface-emitting lasers for data communication and sensing," Photonics Res. **7**(2), 121–136 (2019).
35. A. Rosado, E. P. Martin, A. Pérez-Serrano, J. M. G. Tijero, I. Esquivias, and P. M. Anandarajah, "Optical frequency comb generation via pulsed gain-switching in externally-injected semiconductor lasers using step-recovery diodes," Opt. Laser Technol. **131**, 106392 (2020).
36. C. Abellan, D. Tulli, W. Amaya, and J. Martinez, "Compact Digitization System for Generating Random Numbers," U.S. patent application 17/509, 993 (Feb. 10, 2022).