Research Article Vol. 30, No. 7 / 28 Mar 2022 / Optics Express 10513
Optics EXPRESS

Random polarization switching in gain-switched VCSELs for quantum random number generation

ANA QUIRCE* AND ANGEL VALLE

Instituto de Física de Cantabria (CSIC-Univ. Cantabria), Avda. Los Castros s/n, E39005, Santander, Spain
quirce@ifca.unican.es

Abstract: In this paper, we report an experimental and theoretical study of the random excitation of the linearly polarized modes of a gain-switched VCSEL characterized by having polarization switching under continuous wave operation. We show that equal probability of excitation of both linearly polarized modes can be achieved by adjusting the modulation conditions and the sampling time. Our VCSEL is such that the bistable region associated to the polarization switching is very narrow, indicating that the random process of excitation of the polarizations works independently of the existence of those bistable regions. A characterization of the random polarization switching is performed by analyzing the dependence of the probability of excitation, autocorrelation, and histograms of both polarized signals on the modulation conditions and sampling times. We finally present preliminar results on random number generation using the analyzed system.

1. Introduction

Semiconductor laser modulation is one of the technologies that have enabled the development of versatile and efficient light sources for quantum communications [1]. Several quantum key distribution (QKD) protocols with state-of-the-art performance have been demonstrated using such technologies [1]. Modulated semiconductor lasers can also be used for Quantum random number generation (QRNG) [2–13]. QRNG based on gain-switching modulation of laser diodes is used for high speed random bit generation for state preparation in QKD [1,9,14]. Other applications of QRNG include Monte Carlo simulation, industrial testing, gambling, quantitative finance [2,3], etc. There are also other different strategies for obtaining QRNG [15–24]. The main advantage of QRNGs is that their randomness is inherent to quantum mechanics making these systems a perfect source of entropy for random number generation [3]. The semiconductor lasers that have been used for QRNG are single-mode edge-emitting lasers, typically distributed feedback lasers (DFB). There are several advantages in using modulated edge-emitters for QRNG. They are made of commercially available components and the high signal level permits the use of standard photodetectors. They are simple, fast, robust, have low cost, and operate with flexible clock frequencies.

Vertical-cavity surface-emitting lasers (VCSELs) offer many advantages in comparison to edge-emitters, including high coupling efficiency to optical fibers, low threshold current, single-mode operation, compactness, high energy efficiency, low fabrication costs, ease of 2D array packaging, and on-wafer testing capability [25]. Recent work also shows integration of VCSELs on a silicon photonic integrated circuit [26]. VCSELs usually show two linear orthogonally polarized modes, and polarization switching (PS) between these two orthogonal modes can be observed with temperature or bias current changes [25,27].

A question arises whether PS in VCSELs subject to gain-switching modulation can be used for QRNG. This could be done by applying a periodically modulated current to the VCSEL from a below threshold value to a value above threshold. While the laser is below threshold the optical phases of both linear polarization modes become random due to the spontaneous

#446838 https://doi.org/10.1364/OE.446838
Journal © 2022 Received 26 Oct 2021; revised 28 Dec 2021; accepted 14 Jan 2022; published 15 Mar 2022

Optics EXPRESS

emission noise. More importantly, the linear polarization that emits more power during the initial stages of pulse formation is random because it is determined by the sequence of spontaneous emission noise events. The probability of emission of both linear polarization modes during pulse formation can be similar because both linear polarizations have not very different modal gains and losses. Equalization of both probabilities would be expected when operating with a VCSEL with PS because that point is characterized by similar net gains (gain-losses) for both polarization modes. Random excitation of the VCSEL polarizations can be considered as a quantum entropy source because spontaneous emission events are induced by zero-point oscillations of the electromagnetic field [28,29]. In this way spontaneous emission can be treated as amplified vacuum fluctuations and can be considered as quantum noise [28,29].

To the best of our knowledge only two recent theoretical works [29,30] have discussed the possibility of generating random numbers using the random excitation of polarization modes in a gain-switched VCSEL. This approach has the following advantages: i) it is compact because the basic ingredients are a VCSEL, a polarization beamsplitter and the detection apparatus [29,30], ii) it has "all-optical" functionality, meaning that the final binary random bit streams can be directly obtained at the output port of the VCSEL in real time [30], and iii) it is fast because its ultimate rate is limited by the switching time of the polarization modes, that is similar to the switching time from a non-lasing state of the total laser power [30]. However the starting point of both approaches is the modulation of the VCSEL from the non-lasing state to a polarization bistable regime [29,30]. Although bistable operation is desirable for obtaining that given a particular pulse most of the total power is emitted in one of the two linear polarization modes, it can be a drawback if we want to achieve unbiased operation of the random number generator (that is equal probability for "0" and "1" generated bits). In fact equal probability of occurence of pulses with orthogonal polarizations has only been obtained for specific values of some internal laser parameters: the photon lifetime and the linear birefringence [29] or different fractions of spontaneous emission noise coupled to each polarization mode [30].

In this paper we follow a different approximation to achieve equal probabilities of excitation of the two linearly polarized modes emitted by the gain-switched VCSEL. Our starting point is to consider a VCSEL with PS in continuous wave (cw) operation and to look for the modulation conditions for which unbiased operation can be achieved. We study this problem mainly from an experimental point of view although some results from numerical simulations are also include. We show that the unbiased operation can be easily achieved for a VCSEL with PS. Our VCSEL is such that the bistable region associated to this PS is very narrow. This indicates that our method works independently of the existence of those bistable regions. It has also the advantage of getting unbiased operation for a given device, just by changing the modulation conditions and without changing any of its internal laser parameters.

The paper is organized as follows. In Section 2 we describe the experimental setup and the VCSEL device. Section 3 is devoted to show our experimental results. In Section 4 we present our theoretical model and results. In Section 5 we discuss our results. Finally, in Section 6 the conclusions are summarized.

2. Experimental setup and device characterization

The experimental all-fiber setup is shown in Fig. 1. The optical pulses were generated by gain-switching a VCSEL. This device is a commercially available quantum-well long-wavelength (1550 nm) VCSEL (RayCan), based on InAlGaAs active region. Control of the temperature of the device is performed using a temperature controller (Thorlabs TED200C). The temperature is held constant at 298 K for all the measurements. At this temperature, the threshold current of the VCSEL (I_{th}) is 2.51 mA. The laser is mounted in a laser mount (Thorlabs LDM56M) that includes a bias-tee. The maximum RF modulation frequency is 600 MHz. The laser is driven by the superposition of two electrical signals: a bias current (I_{off}), provided by a current source (Thorlabs

Optics EXPRESS

LDC200C) and a square signal provided by a pulse pattern generator (Anritsu MU181020A). An optical isolator (OI), and FC/APC fiber connectors are used to minimize optical feedback effects in the VCSEL. A polarization controller (PC) and a polarization beamsplitter (PBS) are used to separate the two linear polarization modes of the VCSEL. I_{off} is held constant at a value close to or below threshold for all the measurements. Two fast-photodiodes (9 GHz bandwidth, Thorlabs PDA8GS) were used to transform the optical signals corresponding to each polarization mode to the electrical domain. These signals were recorded in a real-time oscilloscope (13 GHz bandwidth) with a sampling rate of 20 GSa/s to get the temporal profiles of the linearly polarized optical pulses. The output power was also spectrally characterized by means of a high resolution (10 MHz) Brillouin optical spectrum analyzer (BOSA) (Aragon Photonics BOSA 210).

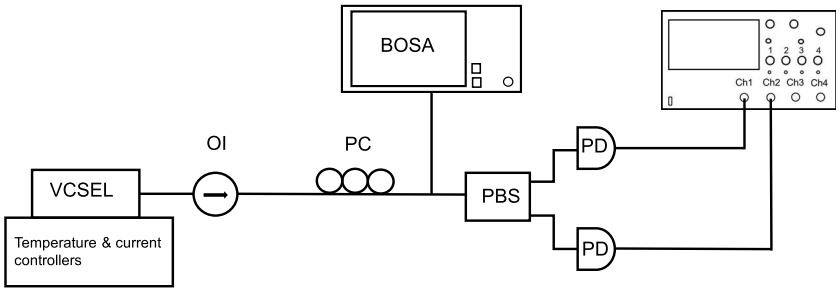

Fig. 1. Schematics of the experimental setup. OI: optical isolator, PC: polarization controller, PBS: polarization beam splitter, PD: photodetector, BOSA: optical spectrum analyzer.

Our VCSEL operates in a single longitudinal and transverse mode over the whole bias current range. The polarization-resolved light-current curve is shown in Fig. 2(a). These measurements correspond to the power measured in both output ports of the PBS. PS from the short-wavelength (labelled as y) to the long-wavelength (x) polarization mode is observed at I_{PS} =6.73 mA bias current value ($I_{PS} = 2.68 I_{th}$). Optical spectrum before and after PS are shown in Fig. 2(b) and Fig. 2(c), respectively. The optical frequency splitting between the y and the x polarizations is 29.8 GHz. A very narrow polarization hysteresis cycle is observed in Fig. 2(a): PS is observed at 6.50 mA when decreasing the bias current. This indicates a polarization bistable region of just 0.23 mA width.

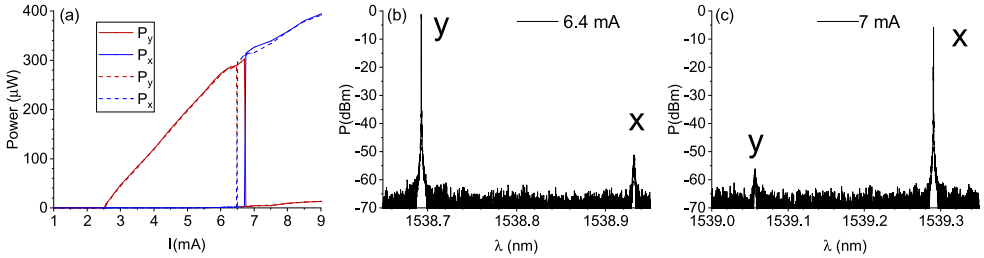

Fig. 2. (a) Polarization-resolved light-current characteristics when increasing (solid lines) and decreasing the current (dashed lines). Optical spectra for a bias current of (b) 6.4 mA, and (c) 7 mA.

3. Experimental results

Our VCSEL is subject to a square wave modulation in which the bias current, I_{off}, is close to or below threshold during $T/2$, and a voltage pulse of constant amplitude V_{on} is applied during the

Optics EXPRESS

rest of the period. Figure 3 shows the temporal waveforms of the $x-$ and $y-$signals measured at the oscilloscope, V_x and V_y, when the bias current is slightly below threshold, I_{off}= 2.5 mA, V_{on}=1.3 V, and T= 10 ns. For these values the injected current while V_{on} is applied is I_{on} = 6.3 I_{th}. Figure 3 shows that the laser switch-offs in all pulses in such a way that there is a random excitation of both linear polarizations after V_{on} is applied (at t = 0). Figure 3 also shows the signal corresponding to the total power. Polarization mode partition noise is observed: both linear polarizations fluctuate in such a way that the fluctuations of the total power are much smaller than those corresponding to the individual polarizations [31]. There are some pulses in which one of the polarizations dominates over the other during all the pulse. In some other pulses there is competition between both polarizations. When this competition appears the $x-$polarization always recovers (see for instance the pulses #1, #3, and #6). We have observed that if T is sufficiently increased V_x always dominates at the end of the voltage pulse with negligible values of V_y. This corresponds to a current applied to the laser that is above the PS current. In this way the $x-$polarization is stable and the $y-$polarization is unstable. This situation is maintained if V_{on}> 0.55 V (I_{on}>I_{PS} = 2.68I_{th}), so this is the voltage amplitude for which PS is achieved when biasing at 2.5 mA.

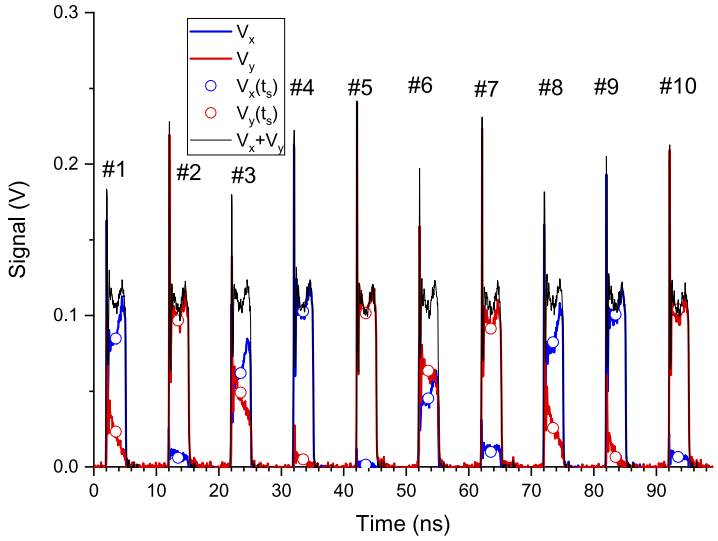

Fig. 3. Experimental time traces of the signals corresponding to the x-polarization (blue line), y-polarization (red line), and total power (black line). The signals at the sampling time are also plotted with symbols. In this figure I_{off} = 2.5 mA, V_{on} = 1.3 V, and t_s = 3.5 ns.

The fact that for long enough T the $x-$polarization always dominates the emission is not an impediment for obtaining random number generation. The key point is to consider small enough values of T for the VCSEL to be always in a transient regime, without letting the device to arrive to its steady state. This is in fact the situation illustrated in Fig. 3. In this way operation in a polarization bistable region is not a requisite for QRNG using the VCSEL polarization, in contrast to [29,30]. Random number generation can be obtained by regularly sampling the $x-$and $y-$signals. Figure 3 shows with symbols the signals (sampled with $1/T$ frequency) at a sampling time, t_s, measured with respect to the time at which V_{on} is applied. The value of t_s in Fig. 3 is 3.5 ns (V_{on} is applied at t = 0 ns). The comparison between $V_x(t_s)$ and $V_y(t_s)$ determines the obtained random bit. In our case we consider that if $V_x(t_s)$>$V_y(t_s)$ ($V_x(t_s) \leq V_y(t_s)$) we obtain a "0" ("1") bit. An alternative way for deciding the bit is to use both outputs of the PBS as inputs into a balanced photodetector. We have checked that this decision process works well with a

Optics EXPRESS

photodetector of 1.6 GHz bandwidth (Thorlabs PDB480C-AC). The decision is simplified since the bit is assigned depending on the positive or negative value of the signal at the sampling time. However in this work we have followed the criterion using two photodetectors since they have much larger bandwidth and permit us to analyze the simultaneous evolution of both linear polarizations.

Figure 4 shows the results of our random number generation process for the conditions considered in Fig. 3. Our results are obtained with 5×10^4 bits. Figure 4(a) shows the probability function of the random sequence of bits. Both probabilities are very close to 0.5, so the bias of this generator can be made very small. Figure 4(b) shows the autocorrelation function of the sequence of 5×10^4 $y-$signal samples up to a delay of 600 samples. The correlation level close to zero for all correlation distances different from zero indicates that the correlation of the obtained random number sequence is small. A very similar autocorrelation function (not shown) is obtained for the $x-$polarized signal. Confidence intervals with 95 % and 99.5 % confidence level are also shown in the figure. The probability density functions (pdf) of the $x-$ and $y-$polarized signals at the sampling time are shown in Fig. 4(c). Both have similar shapes and have local maxima close to the maximum and minimum values of the signals. Of course, this situation appears for the specific sampling time that we have chosen and will significantly change if that time is varied. In Fig. 4(d) we show the pdf of R defined as $R = \max(R_x, R_y)$, where $R_x = V_x(t_s)/(V_x(t_s) + V_y(t_s))$ and $R_y = V_y(t_s)/(V_x(t_s) + V_y(t_s))$. This parameter was introduced in [29] in order to analyze if for a particular pulse the whole power goes into a single polarization mode (this would correspond to R close to 1). The pdf has a maximum at $R = 0.94$ and the averaged value of R is $<R> = 0.803$. This value is similar to the best values obtained theoretically for the bistable operation [29].

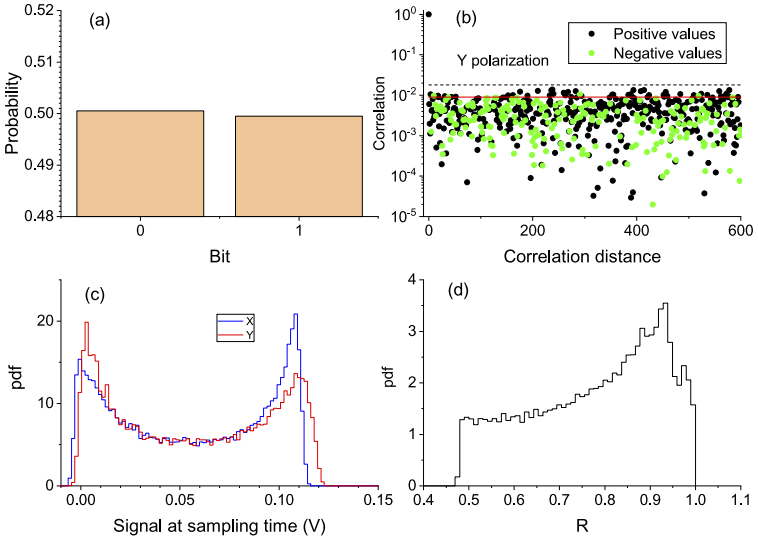

Fig. 4. (a) Histogram, (b) autocorrelation function where black (green) circles correspond to positive (negative) correlation coefficients, (c) histograms of x and y signals at t_s =3.5 ns, and (d) histogram of R evaluated at t_s =3.5 ns. In this figure I_{off} = 2.5 mA, and V_{on} = 1.3 V. The horizontal solid and dashed lines in Fig. 4(b) represent the confidence intervals for the autocorrelation with 95% and 99.5% confidence level.

Some remaining questions about this way of generating random numbers are the sensitivity of the obtained results on the amplitude of the voltage pulse and on the sampling time that is chosen. Results illustrating these dependencies are shown in Fig. 5. We first define the probability of excitation of the $x-$polarization, $P(X>Y)$, as the probability of obtaining $V_x(t_s)>V_y(t_s)$, that is the probability of obtaining a "0" bit. Figure 5(a) shows $P(X>Y)$ as a function of V_{on} for several

Optics EXPRESS

values of the sampling time. $P(X>Y)$ increases when V_{on} increases for all the considered values of t_s. The probability of exciting the $x-$polarization increases with V_{on} because that is precisely the polarization that is excited at large values of the applied current, as it can be seen in Fig. 2(a). This can also be seen in Fig. 6 where time traces corresponding to both linear polarizations are plotted for two values of V_{on}. Figure 6(a) shows that when V_{on} is small, $y-$polarized pulses are preferably excited: $P(X>Y) = 0.23$ when choosing a sampling time at the middle of the pulse ($t_s = 3.5$ ns). The situation is the opposite when increasing V_{on} to 2 V, as it is shown in Fig. 6(b): $x-$pulses are excited with larger probability ($P(X>Y) = 0.61$ for the same value of t_s), in agreement with the results shown in Fig. 5(a).

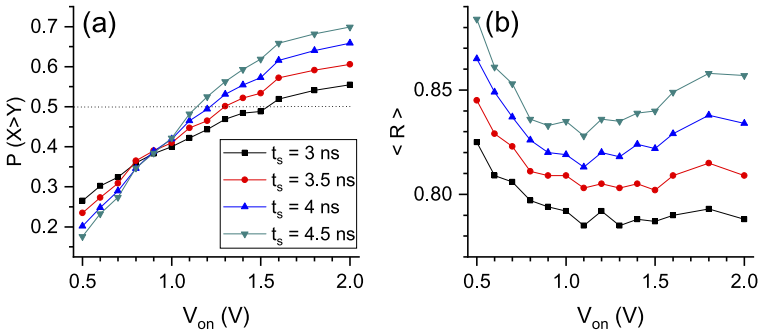

Fig. 5. (a) Probability of excitation of the $x-$polarization as a function of V_{on} for different values of the sampling time. (b) Averaged value of R as a function of V_{on} for different values of t_s. In this Figure $I_{off} = 2.5$ mA.

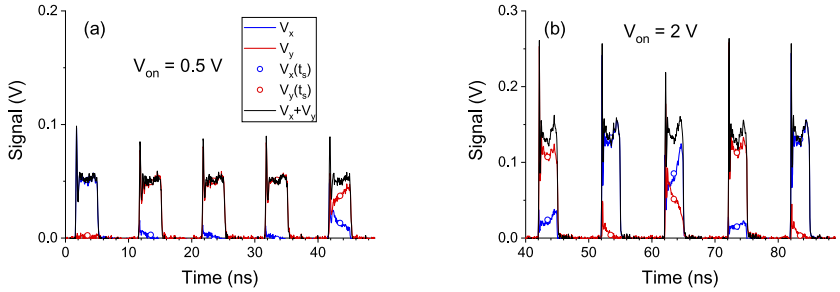

Fig. 6. Experimental time traces of the signals corresponding to the x-polarization (blue line), y-polarization (red line), and total power (black line) for (a) $V_{on} = 0.5V$, and (b) $V_{on} = 2V$ ($I_{on} = 2.47I_{th}$, and $I_{on} = 9.76I_{th}$, respectively). The signals at the sampling time, $t_s = 3.5$ ns, are also plotted with symbols. In this Figure $I_{off} = 2.5$ mA.

The situation illustrated in Fig. 6(b) is similar to that previously discussed in Fig. 3 since in both $I_{on}>I_{PS}$. In contrast, in Fig. 6(a) the situation is the opposite: $I_{on}<I_{PS}$. In this way the polarization that should be always excited at the steady state is the y-polarization (see Fig. 2(a)). In Fig. 6(a) the y-polarization is the one that is excited at the end of the pulse in almost all the cases with the exception of the first pulse. This happens because in Fig. 6(a) the system has not arrived to the steady state yet. During the first pulse the y-polarization is not excited because V_{on} should be applied for a time much longer than 5 ns for letting the $y-$polarization to recover and to arrive to the steady state. In fact, we have also checked (not shown) that the y-polarization is always excited when increasing that time long enough. We note that the time it takes a laser to arrive to the steady state when two modes are competing with very similar gains and losses can be very large, much larger than the time the total power takes to arrive to a constant value, as

Optics EXPRESS

shown in [32]. The main difference between [29,30] and our work is that their VCSELs operate in a bistable regime while our VCSEL does not operate in that regime because the bistable zone is very small, as it can be seen in Fig. 2(a). Bistable operation means that either x or y-polarization pulses can be excited at the steady state. However, as previously discussed, we have not observed this situation.

The dependence of $P(X>Y)$ on the value of t_s illustrated in Fig. 5(a) shows that the range of variation of this probability increases as the sampling time increases. Results included in that figure also show that there is a value of V_{on} for which $P(X>Y)$ does not depend on t_s: $P(X>Y) \sim 0.39$ when $V_{\text{on}} = 0.9$ V ($I_{\text{on}} = 4.3I_{th}$). In order to understand better the evolution of the probability of excitation when changing the value of t_s we have plotted in Fig. 7 the histograms of $V_x(t_s)$ and $V_y(t_s)$ for two different values of t_s for the case illustrated in Fig. 3 and Fig. 4, that is $V_{\text{on}} = 1.3$ V. For this value of V_{on}, Fig. 5(a) shows that $P(X>Y)$ increases when t_s increases. At small values of t_s the $y-$polarization is preferably excited as it can be seen in Fig. 7(a). The range of variation of both, $V_x(t_s)$ and $V_y(t_s)$, is large because the signals are sampled close to the time at which the first spike of the relaxation oscillations is excited (see Fig. 3). Increasing the value of t_s to 3.5 ns lead to similar pdfs for both signal, as it was shown in Fig. 4(c). When t_s is increased to 4.5 ns the $x-$polarization becomes preferably excited as it is shown in Fig. 7(b). This is due to the recovery of the $x-$polarization at the end of the pulse because that polarization is stable, as was discussed in reference to Fig. 3.

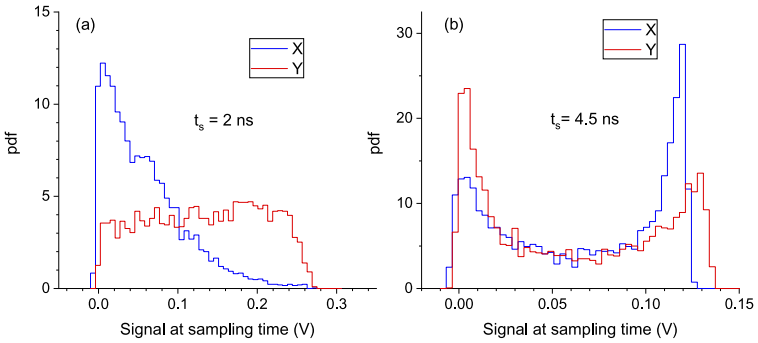

Fig. 7. Histograms of x and y signals at (a) $t_s = 2$ ns, and (b) $t_s = 4.5$ ns. In this Figure $V_{\text{on}} = 1.3V, I_{\text{off}} = 2.5$ mA.

Figure 5(b) shows the dependence of the averaged value of R, $<R>$, on V_{on} for several sampling times. Our results show that there is a value of V_{on} at which $<R>$ is minimum. Figure 5(b) also shows that $<R>$ increases as the sampling time increases. The highest values of $<R>$ are close to 0.885 and are obtained for $t_s = 4.5$ ns and $V_{\text{on}} = 0.5$ V. These are the optimum conditions in our experiment for which most of the power goes to a single polarization.

We now analyze the results obtained when the bias current is below threshold. Figure 8(a) shows the time traces corresponding to both linear polarizations when $I_{\text{off}} = 2.3$ mA and $V_{\text{on}} = 1.4$ V, corresponding to $I_{\text{off}} = 0.92I_{th}$ and $I_{\text{on}} = 6.53I_{th}$, respectively. Similar qualitative behavior to that described when the bias current is very close to threshold is observed. The probability of excitation of the $x-$polarization is close to 0.5 for a similar sampling time to that considered in Fig. 4. The dependence of $P(X>Y)$ on the amplitude of the excitation pulse is shown in Fig. 8(b). This probability increases with V_{on} similarly to the behavior illustrated in Fig. 5(a). Again, as in the case analyzed in Fig. 5, changing V_{on} is a straightforward way of obtaining an unbiased random number generator.

Optics EXPRESS

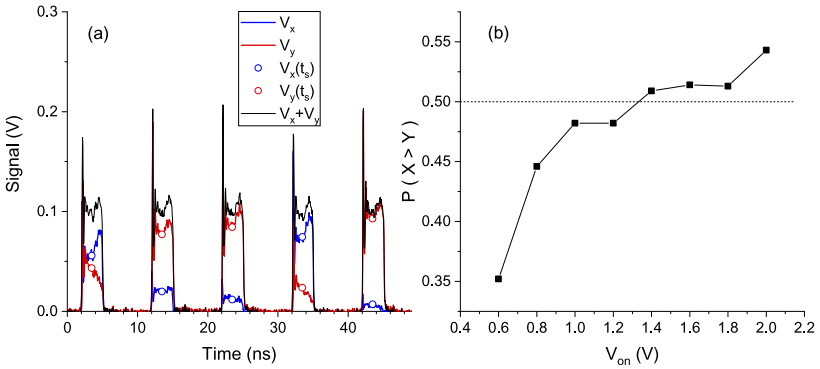

Fig. 8. (a) Experimental time traces of the signals corresponding to the x-polarization (blue line), y-polarization (red line), and total power (black line) for $V_{\text{on}} = 1.4V$. (b) Probability of excitation of the $x-$polarization as a function of V_{on}. In this Figure $I_{\text{off}} = 2.3$ mA, and $t_s = 3.5$ ns.

4. Model and theoretical results

We describe the dynamical evolution of the linear polarization modes of a single-mode VCSEL by using the SFM model [33]. The linearly polarized complex E-fields in the x and y directions are denoted as E_x and E_y, respectively. The other variables are $D = (N - N_t)/(N_{th} - N_t)$ where N, N_{th}, and N_t are the carrier number, carrier number at threshold, and at transparency, respectively, and n, that is the difference of the carriers associated with the spin-up and spin-down levels. The SFM equations modelling VCSELs subject to modulation of the bias current are [33–36]:

$$\frac{dE_x}{dt} = -(\kappa + \gamma_a)E_x - i(\kappa\alpha + \gamma_p)E_x + \kappa(1 + i\alpha)(DE_x + inE_y) + \left(\sqrt{\frac{R_+}{2}}\xi_+(t) + \sqrt{\frac{R_-}{2}}\xi_-(t)\right) \tag{1}$$

$$\frac{dE_y}{dt} = -(\kappa - \gamma_a)E_y - i(\kappa\alpha - \gamma_p)E_y + \kappa(1 + i\alpha)(DE_y - inE_x) + i\left(\sqrt{\frac{R_-}{2}}\xi_-(t) - \sqrt{\frac{R_+}{2}}\xi_+(t)\right) \tag{2}$$

$$\frac{dD}{dt} = \frac{I(t)}{e\,(N_{th} - N_t)} - R(D) - \gamma[D(|E_x|^2 + |E_y|^2) + in(E_yE_x^* - E_xE_y^*)] \tag{3}$$

$$\frac{dn}{dt} = -\gamma_s n - \gamma[n(|E_x|^2 + |E_y|^2) + iD(E_yE_x^* - E_xE_y^*)] \tag{4}$$

where

$$R_\pm = \beta_{SF}\gamma\left[(D \pm n) + \frac{G_N N_t}{2\kappa}\right] \tag{5}$$

$$R(D) = A\Big(D + D_t\Big) + B\Big(D + D_t\Big)^2 + C\Big(D + D_t\Big)^3 \tag{6}$$

, and $D_t = N_t/(N_{th} - N_t)$. We consider an injected current following a square-wave modulation of period T with $I(t) = I_{on}$ during $T/2$, and $I(t) = I_{off}$ during the rest of the period. This modulation is such that $I_{off} < I_{th}$, where I_{th} is the threshold current of the laser, for obtaining a random evolution of the optical phases and power of both linear polarizations induced by the spontaneous emission

Optics EXPRESS

noise. The function $R(D)$ corresponds to the nonlinear carrier recombination. Gaussian white noises, $\xi_+(t)$ and $\xi_-(t)$ are considered to simulate the effect of spontaneous emission noise. Both noises have zero mean $<\xi_i(t)> = 0$ and time correlation given by $<\xi_i(t)\xi_j^*(t')> = \delta(t-t')$ where i, j correspond to subindexes + and -. The parameters γ_a and γ_p are the linear dichroism and the linear birefringence of the VCSEL, respectively. The meaning of the rest of the VCSEL parameters with their corresponding numerical values can be found in Table 1.

Table 1. VCSEL's parameter values

Parameter	Meaning	Value
κ	*Field decay rate*	33 ns^{-1}
γ_p	*Linear birefringence*	103.34 ns^{-1}
γ_a	*Linear dichroism*	- 0.1 ns^{-1}
α	*Linewidth enhancement factor*	2.8
β_{SF}	*Spontaneous emission parameter*	$6.5 \cdot 10^{-4}$
γ	*Decay rate of D*	1.59 ns^{-1}
G_N	*Differential gain*	$1.7 \cdot 10^4 s^{-1}$
N_t	*Carrier number at transparency*	$2.04 \cdot 10^7$
N_{th}	*Carrier number at threshold*	$2.43 \cdot 10^7$
γ_s	*Spin-flip relaxation rate*	1000 ns^{-1}
A	*Nonradiative coefficient*	$2.1 \cdot 10^7$ s^{-1}
B	*Radiative coefficient*	$6.0 \cdot 10^7$ s^{-1}
C	*Auger coefficient*	$7 \cdot 10^6$ s^{-1}

Some of these parameters (γ_p, G_N) have been extracted for the laser of our experiment. The other parameters correspond to a similar 1550-nm wavelength VCSEL characterized in [34] by following the method developed in [34,37] with the exception of some parameters like A, B, and C, that were extracted for another 1550-nm VCSEL in [35]. The theoretical value of I_{th} is 2.6 mA, close to the experimental value.

We show in Fig. 9(a) and Fig. 9(b) the time evolution of the power of the two-linear polarizations of the VCSEL, plotted in logarithmic scale, for different modulation frequencies and I_{off}. The corresponding dynamical evolution of the carrier number normalized by its value at threshold is shown in Fig. 9(c) and Fig. 9(d). Results in Fig. 9 (a),(c) correspond to a 100 MHz modulation frequency and I_{off} slightly below threshold, situation similar to that considered in Fig. 3. This figure shows that spontaneous emission noise dominates the evolution of the photon number in each polarized mode during the laser's switch-off and the initial stages of the laser's switch-on. Figure 9(c) shows that the cavity is depleted of carriers after the laser is switched-off at 125 ns. During that depletion spontaneous emission noise dominates the evolution of both polarization modes in such a way that it rules which linear polarization mode will be preferably excited during the next pulse. We note that this is the case in which the off-current is larger in this work, $I_{\text{off}} = 0.996 I_{th}$, so the effect of spontaneous emission noise will be stronger when I_{off} is smaller (Fig. 8). Therefore in the experimental cases that we have considered the RF modulation is such that the off time is long enough and at a low enough current for the spontaneous emission to rule the next emission event.

Our model does not consider any fluctuations in the VCSEL bias current and gives qualitatively the same polarization switching results than in the experiment. Therefore the generation of random numbers in our experiment comes from the polarization switching, and not from the variations in current which are inherent from the driving of the electrical circuit, like jitter or current noise.

Optics EXPRESS

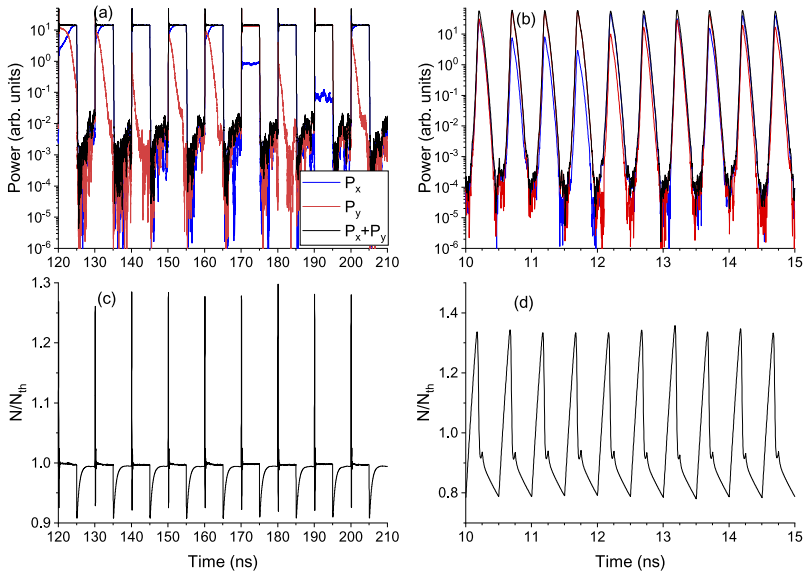

Fig. 9. (a)-(b) Simulated time traces of the power of x (blue line) and y (red line) polarization modes. The total power is also plotted with black lines. (c)-(d) Simulated time traces of the ratio between the carrier number and carrier number at threshold. In (a),(c) the modulation frequency is 100 MHz, $I_{on} = 6.3I_{th}$, $I_{off} = 0.996I_{th}$. In (b),(d) the modulation frequency is 2 GHz, $I_{on} = 6.3I_{th}$, $I_{off} = 0$.

5. Discussion

The modulation frequency considered up to now in our experiment is not very fast, 100 MHz. Experimental results obtained for a higher modulation frequency, 200 MHz, are shown in Fig. 10. Time traces of the signals corresponding to both linear polarizations when $P(X>Y)$ is close to 0.5 are shown in Fig. 10(a). The dependence of $P(X>Y)$ on V_{on} is also shown in Fig. 10(b). Again, similar qualitative behavior to that described for smaller modulation frequencies is observed. Modulation rates in our experiment are limited by the maximum RF modulation frequency of our laser mount. To show that the random number generation process can go beyond the considered frequencies we have obtained theoretical results when the modulation frequency is 2 GHz. Results are shown in Fig. 9(b) and Fig. 9(d). While the value of I_{on} is similar to that in Fig. 9(a), the value of I_{off} has been decreased to zero in order to randomize the evolution of both linear polarizations before the next emission event. Our results confirm that random excitation of both linear polarizations is also obtained at modulation frequencies much higher than those considered in our experiments.

The speed of QRNGs based on PS in VCSELs would be limited by the switching times of the polarization modes. With the usual definition of switching time (time at which the power crosses a prescribed fixed level) the switching time for the total power is very similar to that of the excited polarization mode, providing that most of the power is emitted in that mode. If both polarization modes are excited during the rising edge of the pulse, the switching time of the total power is slightly smaller that those corresponding to individual polarizations. In any case the switching time for the polarizations is similar to that corresponding to the total laser power, and hence the speed of the random generator is limited by the current modulation bandwidth of the VCSEL. Continuous improvements in this bandwidth have been obtained motivated by the use of VCSELs for data communications [38]. Modulation bandwidths beyond 35 GHz and data rates beyond 50 Gbps in the on–off keying modulation format have been demonstrated [38]. Future

Optics EXPRESS

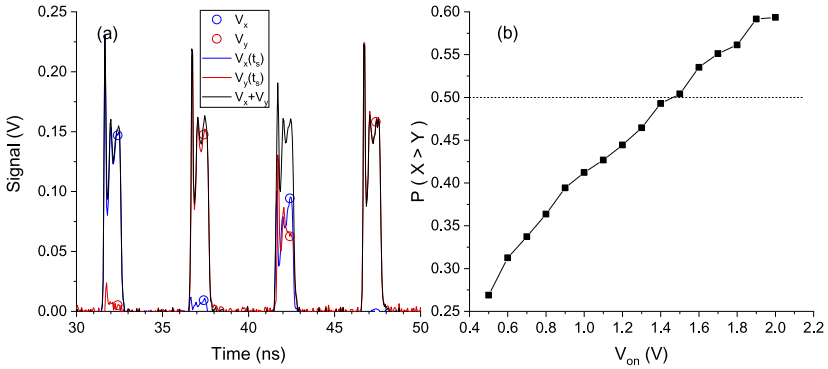

Fig. 10. (a) Experimental time traces of the signals corresponding to the x-polarization (blue line), y-polarization (red line), and total power (black line) for $V_{\text{on}} = 1.5V$. (b) Probability of excitation of the $x-$polarization as a function of V_{on}. In this Figure the modulation frequency is 200 MHz, $I_{\text{off}} = 2.5$ mA, and $t_s = 2.4$ ns.

work is planned on increasing the bit rate of our generator. Also a detailed comparison of our experimental results with those obtained with the theory would permit to characterize better this type of QRNG. This comparison will be performed by using the complete set of extracted parameters for our VCSEL following the procedure developped in [34,37].

In this work we have focused on describing the random polarization switching obtained when gain-switching a VCSEL with PS under cw operation. Periodic modulation of the bias current applied to the device and the effect of spontaneous emission noise induce random PS. In this way unbiased random generators can be obtained just by changing the parameters of the modulation. We note that in order to minimize bias in these type of generators a feedback loop applied on the voltage could be necessary for maintaining a constant value of V_{on}. In these generators randomness increases as the bias current is decreased below threshold. In our study we have analyzed two cases: $I_{\text{off}} \sim I_{th}$ and $I_{\text{off}} = 0.92 I_{th}$ for which we have obtained an unbiased generator by tuning the pulse amplitude and the sampling time. Unbiased operation for smaller values of I_{off} can be obtained by increasing the values of the pulse amplitudes. The value of V_{on} for which unbiased operation is obtained also depends on the current at which PS is obtained under cw operation, I_{PS}. For our device PS is obtained at I_{PS} =2.68 I_{th}. Using VCSEL devices with smaller values of I_{PS} is a strategy for obtaining unbiased operation for smaller values of I_{off} and similar excitation levels to those used in this work. Changing I_{PS} for a given VCSEL can be done by applying anisotropic strain to the device [39]. A simpler way of changing I_{PS} for a given device is by modifying the temperature of operation [27,40]. Unfortunately we could not use this method in our VCSEL because the change of I_{PS} with the temperature is small, that is an indication of the non-thermal origin of our PS [40].

The process of generating random bits in our system is based on sampling the signals corresponding to both linear polarizations in such a way that the time between consecutive samples corresponds to the modulation period. If the signal corresponding to the $x-$polarization is larger than that corresponding to the $y-$polarization we assign a "0" bit, otherwise a "1" bit is obtained. In this way bit streams have been obtained, for instance the 5×10^4 bit stream that has been used in Fig. 4. We have repeated the experiment of Fig. 4 several times several weeks apart, just by using the same parameters and without adjusting any setup parameter. Results obtained with streams of 5×10^4 bits have been very similar. In the experiments the obtained biases of the random number generator, b =(Probability("0") - Probability("1"))/2, have been of the order of $\pm 10^{-3}$. This indicates the good repeatibility of our experiment.

Optics EXPRESS

We have also repeated the experiment under the same conditions but increasing the number of data, from 5×10^4 to 2.5×10^6 bits. We have considered a post-processing of our data by using the von Neumann algorithm described in [2] to obtain a data set of 6.2×10^5 bits. The post-processed bit string has a bias of -1.04×10^{-4} and a min-entropy value of 0.9997 per bit. We have also done an initial study in order to test the randomness of our data. As a preliminar step we have splitted the 6.2×10^5 bits in five sequences of 1.24×10^5 bits each. All these sequences pass a chi-square test of goodness-of-fit with a 0.01 level of significance [41]. The second step has been to use the 6.2×10^5 bits sequence as input for the NIST SP800-22 statistical test suite with a 0.01 level of statistical significance [42]. The sequence of 6.2×10^5 bits passes all the NIST tests. However, since the bit number is small, we have been able to calculate the proportions of sequences that pass the tests only for those that can work with short bit streams. P-values and proportions are shown in Fig. 11 for the experimental conditions of Fig. 3. Averaged P-values and proportions are calculated using 1000 sequences of 625 bits each for the Frequency test, Frequency within a block, Runs test, Longest-Run-of-Ones in a Block, and Cumulative sums forward and backward. The same calculations have been done for the FFT test but using 500 sequences of 1250 bits. For the other tests we plot the results using only the sequence of 6.2×10^5 bits, and therefore no data on proportions are included in Fig. 11. The distributions of P-values for the tests for which we have calculated proportions are rather uniform. Averaged P-values are around 0.5 and the range of the standard deviation of the P-values goes from 0.288 (Frequency within a block) to 0.307 (FFT test). We are aware that the number of analyzed data is small and more work has to be done in order to collect a sufficient number of data to fully pass batteries of statistical tests like NIST SP800-22. Anyway we think that these preliminar results indicate that our system can be a good candidate for random number generation.

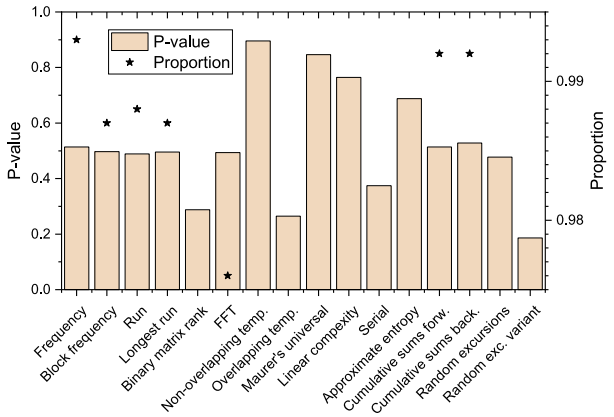

Fig. 11. NIST test results for a modulation frequency of 100 MHz, $I_{\text{off}} = 2.5$ mA, $V_{\text{on}} = 1.3$ V and $t_s = 3.5$ ns. Tests without star correspond to those run with one long sequence, then no proportion data are given.

Our method for random number generation and those based in DFB lasers share some characteristics. In both methods a semiconductor laser is gain-switched with a bias current below threshold. Also both methods rely on the random characteristics of the spontaneous emission while the laser is below threshold. However, while QRNGs that use DFBs are based on the random character of the optical phase of the pulses and the polarization of the light plays no role because the laser maintains its linear polarization, our generator is based on the random excitation of the linear polarizations of the VCSEL. Another important difference between our all-optical approach and those using DFB lasers is that we do not need an unbalanced Mach-Zehnder

Optics EXPRESS

interferometer to convert phase fluctuations into the amplitude fluctuations that, adequately sampled and postprocessed, generate the random numbers.

6. Summary and conclusion

Summarizing, we have analyzed in an experimental and a theoretical way the random excitation of the linear polarization modes of a gain-switched VCSEL characterized by having PS under cw operation. Our VCSEL is such that the bistable region associated to the polarization switching is very narrow, indicating that our generator works independently of the existence of those bistable regions. We have characterized the random excitation of the polarized modes by measuring how the probability of excitation, autocorrelation, and histograms corresponding to each linear polarization depend on the modulation conditions and sampling times. We have demonstrated that equal probability of excitation of both linear polarization modes can be achieved by adjusting the modulation conditions and the sampling time. In this way there is no need of changing any of the internal VCSEL parameters to get an unbiased operation of a random number generator based on this system. A good qualitative agreement between our experimental and theoretical results has been obtained, as seen from the comparison of Fig. 3 and Fig. 9(a). Future work will be devoted to a complete extraction of the VCSEL parameters in order to perform a quantitative comparison between the results of our model and experiments, as it has been done previously for gain-switched edge-emitting laser diodes for QRNG [13,43]. This comparison is useful for selecting optimal parameters to maximize the QRNG performance and monitor the device behavior to detect malfunctioning of the device [43]. In this work we have presented preliminar results on random number generation based on gain-switching VCSELs. We are aware that we do not have a random number generator yet because much more data must be collected in order to fully pass several batteries of statistical tests. Our main intention has been to present and analyze in detail the random polarization switching in VCSELs that can make this device become a candidate for random number generation.

Funding. Ministerio de Ciencia, Innovación y Universidades (RTI2018-094118-B-C22 MCIN/AEI/FEDER, UE).

Acknowledgments. A. Quirce acknowledges financial support from Beatriz Galindo program, Ministerio de Ciencia, Innovación y Universidades (Spain). We thank Jaime Gutiérrez, Marcos Valle Miñón, and Iván Rivero for their help in the calculations.

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. 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).
2. M. Stipčević and Ç. K. Koç, "True random number generators," in *Open Problems in Mathematics and Computational Science*, (Springer, 2014), pp. 275–315.
3. M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum random number generators," Rev. Mod. Phys. **89**(1), 015004 (2017).
4. 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).
5. 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).
6. 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).
7. 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).
8. 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).

Optics EXPRESS

9. 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).
10. 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).
11. 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).
12. R. Shakhovoy, A. Tumachek, N. Andronova, Y. Mironov, and Y. Kurochkin, "Phase randomness in a gain-switched semiconductor laser: stochastic differential equation analysis," arXiv preprint arXiv:2011.10401 (2020).
13. A. Quirce and A. Valle, "Phase diffusion in gain-switched semiconductor lasers for quantum random number generation," Opt. Express **29**(24), 39473–39485 (2021).
14. K. Nakata, A. Tomita, M. Fujiwara, K.-I. Yoshino, A. Tajima, A. Okamoto, and K. Ogawa, "Intensity fluctuation of a gain-switched semiconductor laser for quantum key distribution systems," Opt. Express **25**(2), 622–634 (2017).
15. 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).
16. M. Stipčević and B. M. Rogina, "Quantum random number generator based on photonic emission in semiconductors," Rev. Sci. Instrum. **78**(4), 045104 (2007).
17. H. Fürst, H. Weier, S. Nauerth, D. G. Marangon, C. Kurtsiefer, and H. Weinfurter, "High speed optical quantum random number generation," Opt. Express **18**(12), 13029–13037 (2010).
18. W. Wei and H. Guo, "Bias-free true random-number generator," Opt. Lett. **34**(12), 1876–1878 (2009).
19. 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).
20. 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).
21. 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).
22. 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).
23. 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).
24. 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).
25. R. Michalzik, *VCSELs: fundamentals, technology and applications of vertical-cavity surface-emitting lasers*, vol. 166 (Springer, 2012).
26. E. Haglund, M. Jahed, J. S. Gustavsson, A. Larsson, J. Goyvaerts, R. Baets, G. Roelkens, M. Rensing, and P. O'Brien, "High-power single transverse and polarization mode vcsel for silicon photonics integration," Opt. Express **27**(13), 18892–18899 (2019).
27. 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).
28. R. Loudon, *The quantum theory of light* (OUP Oxford, 2000).
29. 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).
30. J. Zhao, P. Li, X. Zhang, Z. Gao, Z. Jia, A. Bogris, K. A. Shore, and Y. Wang, "Fast all-optical random number generator," preprint, available at https://www.researchgate.net/publication/342123170.
31. A. Valle, M. Sciamanna, and K. Panajotov, "Irregular pulsating polarization dynamics in gain-switched vertical-cavity surface-emitting lasers," IEEE J. Quantum Electron. **44**(2), 136–143 (2008).
32. A. Valle, A. Mecozzi, L. Pesquera, M. A. Rodríguez, and P. Spano, "Transient statistics for two mode gas ring lasers," Phys. Rev. A **48**(3), 2426–2432 (1993).
33. J. Martin-Regalado, F. Prati, M. San Miguel, and N. B. Abraham, "Polarization properties of vertical-cavity surface-emitting lasers," IEEE J. Quantum Electron. **33**(5), 765–783 (1997).
34. P. Pérez, A. Valle, and L. Pesquera, "Polarization-resolved characterization of long-wavelength vertical-cavity surface-emitting laser parameters," J. Opt. Soc. Am. B **31**(11), 2574–2580 (2014).
35. A. Quirce, C. de Dios, A. Valle, L. Pesquera, and P. Acedo, "Polarization dynamics in VCSEL-based gain switching optical frequency combs," J. Lightwave Technol. **36**(10), 1798–1806 (2018).
36. A. Quirce, C. de Dios, A. Valle, and P. Acedo, "VCSEL-based optical frequency combs expansion induced by polarized optical injection," IEEE J. Sel. Top. Quantum Electron. **25**(6), 1–9, Art no. 1500109, (2019).
37. P. Pérez, A. Valle, I. Noriega, and L. Pesquera, "Measurement of the intrinsic parameters of single-mode vcsels," J. Lightwave Technol. **32**(8), 1601–1607 (2014).
38. 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).

Optics EXPRESS

39. K. Panajotov, B. Nagler, G. Verschaffelt, A. Georgievski, H. Thienpont, J. Danckaert, and I. Veretennicoff, "Impact of in-plane anisotropic strain on the polarization behavior of vertical-cavity surface-emitting lasers," Appl. Phys. Lett. **77**(11), 1590–1592 (2000).
40. A. Quirce, A. Valle, L. Pesquera, H. Thienpont, and K. Panajotov, "Measurement of temperature-dependent polarization parameters in long-wavelength vcsels," IEEE J. Sel. Top. Quantum Electron. **21**(6), 636–642 (2015).
41. M. H. DeGroot and M. J. Schervish, *Probability and Statistics*, (Addison-Wesley, 2012).
42. A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo, "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications," NIST Special Publication, 800, 22 (2010).
43. 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).