Characterization of the Polarization Fluctuations in Gain-Switched VCSELs for Quantum Random-Number Generation

ANA QUIRCE,[1], ANGEL VALLE[1,*], MARCOS VALLE-MIÑÓN[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 report a characterization of the polarization fluctuations observed when gain-switching vertical-cavity surface-emitting lasers (VCSELs) for quantum random number generation (QRNG) applications. We compare our experimental measurements with the results obtained from a stochastic rate equations model that incorporates the intrinsic parameters of the VCSEL found using the state-of-the-art experimental techniques. The good agreement obtained between our experiments and simulations can be used to establish a validation process that permits to monitor the device behaviour to detect malicious intrusion or malfunctioning of the QRNG. Simulations of the model are used to look for parameters that maximize the QRNG performance. Along this direction we consider the performance when considering a VCSEL with vanishing values of the amplitude and phase anisotropies. We show that in this system the obtained raw bits have a low bias value that is independent on the sampling time chosen to obtain the random bit and on the parameters of the modulation. We also use the simulations of the model to predict the QRNG performance at high modulation frequencies. We show that random bits obtained at several Gbps rates, after appropriate post-processing, fully pass the NIST statistical test.

1. Introduction

Weak coherent pulses (WCPs), obtained from attenuation of semiconductor laser pulses, are used as single photon sources in most commercial and research Quantum Key Distribution (QKD) systems from early 1990s [1, 2]. Several QKD protocols with state-of-the-art performance have been demonstrated using WCPs [2]. Pulses of light generated by gain-switched semiconductor lasers have random phases because of the random character of the phase of the spontaneous emission photons that seed these pulses during their formation. Random-phase pulses emitted by gain-switched semiconductor lasers also find applications in quantum random number generation (QRNG) [3–7]. QRNGs stand out from hardware physical random number generators because their randomness stems from quantum processes, this being the best guarantee for offering optimum privacy and security while maintaining high performance [3–10]. There are many other different strategies for obtaining QRNG apart from phase-noise QRNGs. Device-independent randomness expansion using entangled photons [11] and source-independent QRNGs [10, 12] have been recently described. QRNGs based on the detection of single-photon events [13–17] and multiphoton QRNGs [18–34] have been demonstrated. QRNGs find applications including cryptography [9, 35], Monte Carlo simulations [36], weather prediction , quantitative finance [8], data processing [8], industrial testing [8], gambling [37], fundamental Physics tests [37] etc. Specific applications of QRNGs can also be found in fundamental physics tests and particularly

in quantum communications because using these generators is a necessary security requirement for QKD [2].

Two main types of semiconductor lasers have been used in the gain-switching regime for QRNG: edge-emitters and vertical-cavity surface-emitting lasers (VCSELs). In edge-emitters based QRNGs, pulses of light with random phases and similar amplitudes are generated by periodic gain-switching of a single-mode laser (typically a distributed feedback laser) from below to above its threshold. Large phase fluctuations induced by spontaneous emission appear when the laser is biased below threshold. Spontaneous emission is a mechanism that generates quantum fluctuations, as it can be ascribed to the vacuum fluctuations of the optical field [21, 38]. Phase fluctuations can be converted into amplitude fluctuations by using an unbalanced Mach-Zehnder interferometer [24, 25]. From these amplitude fluctuations random numbers are obtained after proper digitization. Advantages of these QRNGs include fast operation at Gbps rates (up to 68 Gbps [26]), multi-clock frequency flexibility, simplicity, robustness, low cost, the high signal level that permits the use of standard photodetectors, and the integration on an InP platform [27].

VCSELs offer several advantages in comparison to edge-emitters, including lower fabrication costs, high coupling efficiency to optical fibers, lower threshold current, single longitudinal mode operation, compactness, high energy efficiency, ease of 2D array packaging, and on-wafer testing capability [39]. Recent work has shown micro-transfer-printing of bottom-emitting VCSELs on silicon nitride photonic integrated circuits enabling scalability towards low-cost and large-volume production [40]. VCSELs usually show two orthogonal linearly polarized modes in such a way that polarization switching (PS) between them can be observed when changing the temperature or the bias current applied to the device [39, 41].

Gain-switching of VCSELs has also been used for QRNG because when the applied bias current is modulated from below to above the threshold value the linearly polarized mode that is preferably excited is random since it is determined by the sequence of spontaneous emission noise events [33, 42–48]. QRNGs based on VCSELs have the advantages of low fabrication cost, small size, compactness, and simplicity (coherent detection is not required). Since the initial demonstration by Chizhevsky of random number generation based on the fluctuations of the linearly polarized modes when gain-switching the VCSEL [42] just a few theoretical [44–47] and experimental analysis [33, 43, 46, 48] have been performed. In Ref. [33] a large random bit stream was experimentally obtained that, after appropriate post-processing, fully passed all tests in the standard test suite for random number generators provided by the National Institute of Standards and Technology (NIST) [49].

QRNGs based on edge-emitters or VCSELs belong to the class of trusted-device QRNGs [4]. In these systems it is very useful to build a model of the physical entropy source to guarantee unpredictability, in the sense that the device is generating randomness of genuine quantum origin [32]. In gain-switched edge-emitter lasers the results of numerical simulations of the stochastic rate equations that quantify the phase noise have been compared with the experimental results for validating the operational limits of the phase-noise QRNG [32]. This validation process can be used to check the device performance in order to detect malfunctioning or malicious manipulation of the QRNG [32]. A good quantitative description of experimental phase noise using stochastic rate equation modelling can only be obtained when extraction of the parameters of the semiconductor laser is performed [32, 50]. To the best of our knowledge a similar validation process for QRNGs based on gain-switching VCSELs has not been performed yet.

In this work we characterize the polarization fluctuations found in gain-switched VCSELs by comparing experimental measurements with the results obtained from a stochastic rate equations model that incorporates the VCSEL's intrinsic parameters found using the state-of-the-art experimental techniques [51–53]. The good agreement found between our experiments and simulations is a solid step towards establishing a validation process similar to that defined for QRNGs based on gain-switched edge-emitters [32]. The model can be used to detect malfunctioning of the

QRNG and to select optimal parameters to maximize the QRNG performance. We note that the comparison between experimental and theoretical results was not performed in [46]. We show that a current-dependent linear dichroism must be considered in the simulations for obtaining a good quantitative agreement between experimental and theoretical results. This dependence was not considered in [46]. We also theoretically analyze a situation, not considered in [46], in which a VCSEL with vanishing values of the amplitude and phase anisotropies is used as entropy source in order to optimize the QRNG performance. We show that in this system the obtained raw bits have a low bias value that is independent on the sampling time chosen to obtain the random bit and on the parameters of the modulation. Finally, we also use the model to predict the QRNG performance at high modulation frequencies, values that are beyond our experimental capabilities. We extend the initial theoretical results obtained in [46] to predict that the probability of excitation of a given polarization mode depends on the linear birefringence parameter. We show that random bits obtained at several Gbps rates fully pass the NIST test after appropriate post-processing, extending in this way the results obtained in [33] for 100 Mbps.

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 theoretical model. In Section 4 we present our comparison between theoretical and experimental results. In Section 5 we present the theoretical results for a VCSEL with no anisotropies. Section 6 is devoted to describe the QRNG performance at high modulation frequencies. Finally, in Section 7 the conclusions are summarized.

2. The experiment

The experimental all-fiber setup is shown in Fig. 1. A quantum-well VCSEL (Raycan) based on InAlGaAs active region and emitting close to a wavelength of 1550 nm is used in our experiments. The same laser was used in [33, 46, 48]. The nominal modulation bandwidth of the VCSEL is 2.5 GHz. The VCSEL is mounted in a laser mount (Thorlabs LDM56M) that includes a bias-tee. This mount has a maximum RF modulation frequency of 600 MHz. The VCSEL is gain-switched by applying a superposition of two electrical signals: a constant bias current , $I_{\rm off}$, provided by a current source (Thorlabs LDC200C), and a radiofrequency (RF) square signal provided by a pulse pattern generator (Anritsu MU181020A). A temperature controller (Thorlabs TED200C) is used to keep a constant temperature of the laser, 25 ^{o}C, during all the experiments. At this temperature, the threshold current of the VCSEL, $I_{\rm th}$, is 2.51 mA. An optical isolator (OI), is used to minimize optical feedback effects in the VCSEL. A polarization controller (PC) is combined with a polarization beamsplitter (PBS) to separate the two linearly polarized modes of the VCSEL. Two fast-photodetectors that include an amplification stage (Thorlabs PDA8GS, 9 GHz bandwidth) are used in combination with a real-time high-speed oscilloscope (13 GHz bandwidth) to measure the signal corresponding to each linearly polarized mode.

The VCSEL emits in a single longitudinal and transverse mode over the whole bias current range. However a polarization switching (PS) from the short-wavelength (labelled as $y-$polarization) to the long-wavelength (labelled as x) linearly polarized mode appears when increasing the bias current. The PS is illustrated in Fig. 2 of Ref. [46] in which the polarization-resolved light-current characteristics and the optical spectrum before and after PS are shown. The optical frequency splitting between the y and the x linear polarizations is $\nu_y - \nu_x = 29.8$ GHz. The bias current at which PS is observed, $I_{\rm PS}$, is 6.73 mA (6.50 mA) when increasing (decreasing) that current. This narrow hysteresis cycle indicates that the bistable behavior of the linear polarizations is only observed in a very small current range (0.23 mA width).

The VCSEL is gain-switched by applying a square-wave modulation of period T. A constant bias current ($I_{\rm off}$, such that $I_{\rm off} < I_{\rm th}$) and a periodic voltage, $V(t)$, such that $V(t) = V_{\rm on}$ during half of the period and $V(t) = 0$ during the rest of the period) are applied to the bias-tee. Fig. 2 shows the time traces of the $x-$ and $y-$signals measured at the oscilloscope, V_x and $V_{\rm y}$, when the bias current is slightly below threshold, $I_{\rm off} = 2.5$ mA, $V_{\rm on} = 1.3$ V, and $T = 10$ ns (that corresponds

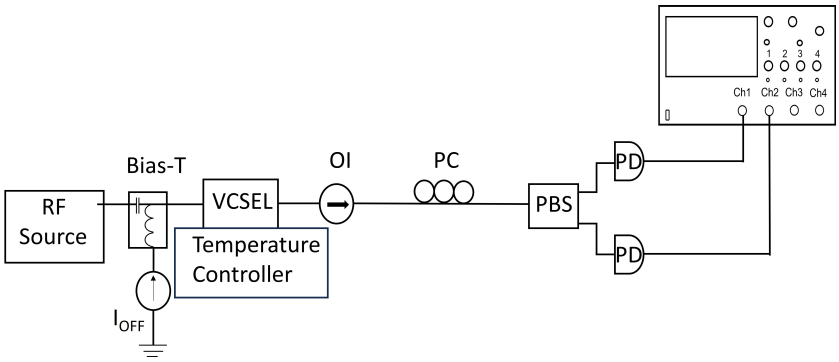

Fig. 1. Schematics of the experimental setup. OI: optical isolator, PC: polarization controller, PBS: polarization beam splitter, PD: photodetector, OSC: oscilloscope.

to a modulation frequency, f_{mod}, of 100 MHz). V_x and V_y are proportional to the power of the $x-$ and $y-$linearly polarized modes. The VCSEL switches-off in all the cycles in such a way that there is a random excitation of both linearly polarized modes induced by spontaneous emission noise. Fig. 2 also shows that the total power, proportional to $V_x + V_y$, fluctuates much less than the individual linear polarizations [46, 54]. There are some pulses in which one of the polarizations dominates over the other during all the pulse (see for instance the pulses #2, #3, and #10). In some other pulses there is a strong competition between both polarizations (see for instance the pulses #1, and #4).

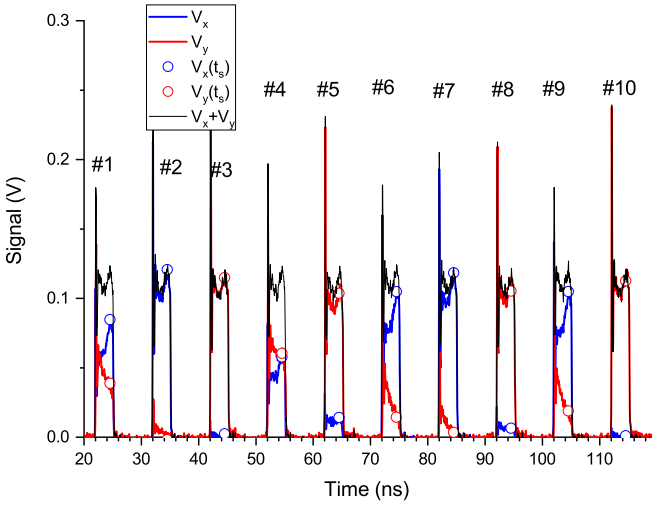

Fig. 2. Experimental time traces of the signals corresponding to the x-polarization (blue line), y-polarization (red line), and total power (black line). The signals at the sampling time are also plotted with symbols. $f_{\text{mod}} = 100$ MHz, $I_{\text{off}} = 2.5$ mA, $V_{\text{on}} = 1.3$ V, and $t_s = 4.5$ ns.

One way of obtaining random numbers from the above mentioned polarization fluctuations is by regularly sampling the $x-$and $y-$signals at a sampling time, t_s, measured with respect to the beginning of each modulation cycle. We consider that each modulation cycle begins when

V_{on} is applied (for instance, t = 20 ns for the first cycle in Fig. 2). In this way for the m cycle the signals are sampled at $t_m = t_s + mT$ where m=0,1... is a natural number. We also show in Fig. 2 the regularly sampled signals, $V_x(t_s)$ and $V_y(t_s)$ (see blue and red circles, respectively). The comparison between $V_x(t_s)$ and $V_y(t_s)$ is one way for determining the obtained random bit. 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, in a way similar to [46].

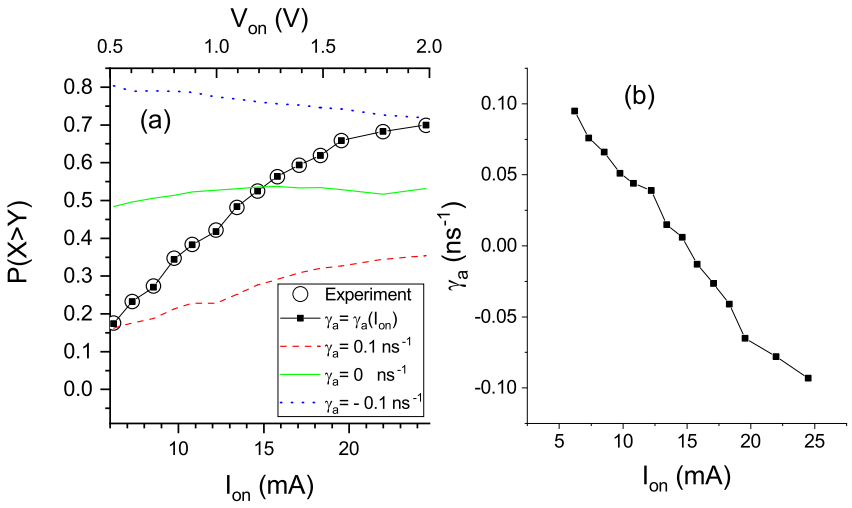

Fig. 3. (a) Probability of excitation of the $x-$ polarization as a function of I_{on} and V_{on} for f_{mod} = 100 MHz, I_{off} = 2.5 mA, and t_s = 4.5 ns. Experimental and simulated values are plotted with circles and solid lines, respectively. (b) Linear dichroism as a function of I_{on} for which the simulated results of part (a) are obtained.

In order to quantify the probability of obtaining a certain bit, we 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, $p(0)$. Fig. 3(a) shows with circles that probability as a function of V_{on} and as a function of the current when V_{on} is applied, I_{on}. The modulation and sampling conditions are those of Fig. 2. Each of the points has been obtained with 10^4 bits. The relation between I_{on} and V_{on} has been obtained by using the V-I curve since the modulation frequency is small. $P(X > Y)$ increases when I_{on} increases because the $x-$linearly polarized mode is excited at large values of the applied current in cw-operation [46]. The remaining experimental results will be presented in Section 4 when compared with the theoretical results.

3. The Model

In this section we present the theoretical model, the Spin Flip Model (SFM), that describes the dynamical evolution of the linearly polarized modes of a single-mode VCSEL [55]. The linearly polarized complex electric fields in the x and y directions are $E_x(t)$ and $E_y(t)$, respectively. There are two carrier variables. The first one is $D(t) = (N(t) - N_t)/(N_{th} - N_t)$ where $N(t)$, N_{th}, and N_t are the carrier number, carrier number at threshold, and carrier number at transparency, respectively. The second one is $n(t)$, that is the difference of the carriers associated with the

spin-up and spin-down levels. The rate equations that describe the dynamical evolution of those variables are [52, 53, 55, 56]

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

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

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

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

where

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

$$R(D) = A\Big(D + D_t\Big) + B\Big(D + D_t\Big)^2 + C\Big(D + D_t\Big)^3, \quad (6)$$

and $D_t = N_t/(N_{\rm th} - N_t)$.

The function $R(D)$ corresponds to the non-linear carrier recombination. In our simulations the injected current, I, follows a square-wave modulation of period T, i.e., $I(t) = I_{\rm on}$ during $T/2$, and $I(t) = I_{\rm off}$ during the rest of the period. 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. Within the framework of the SFM, the γ_a parameter is essential to describe the polarization behavior of the VCSEL [39]. This parameter can be measured from the difference between the spectral widths of the two linear polarizations [52, 57]. The measurement of this parameter under cw-operation has shown that it depends on the bias current [52, 58] and therefore we consider in our model that $\gamma_a = \gamma_a(I_{\rm on})$. That dependence is illustrated in Fig. 3 of Ref. [52] in which γ_a is shown to decrease linearly with $I_{\rm on}$ when $I_{\rm on} \sim I_{\rm PS}$ for another VCSEL that has a polarization behavior similar to that described in the previous section. The meaning of the rest of the VCSEL's parameters can be found in Table 1.

4. Comparison between theoretical and experimental results

In order to perform a comparison between our experimental results and the results of the theoretical model an extraction of the intrinsic parameters of the VCSEL is desirable. The parameters of our VCSEL are obtained using the techniques described in [51–53] in which high resolution cw-optical spectrum measurements are the basis of the extraction process. The numerical values of the VCSEL parameters are included in Table 1. Using these parameters we have integrated numerically Eqs. (1)-(4) using the Euler-Maruyama method [59, 60] with an integration time step of 0.05 ps.

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*	variable
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*	2100 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}

We first show the theoretical results obtained for $P(X > Y)$ when γ_a is constant and independent of I_{on}. Fig. 3(a) shows the simulated results for three different values of γ_a (0.1, 0, and -0.1 ns^{-1}) when using the same experimental conditions considered in Fig. 3(a). This figure shows that we can not get a good agreement between experimental and theoretical results when using a single γ_a value. So as to get that agreement we need to consider the dependence of γ_a on I_{on}. Fig. 3(b) shows the value of γ_a that must be considered for each value of I_{on} in order to get that good agreement. We note that γ_a is then considered as a fitting parameter since we do not measure it directly. We follow this procedure because if we consider the $\gamma_a = \gamma_a(I_{\text{on}})$ relation obtained with the measurement procedure of Refs. [52, 57] we do not get a good agreement. This is because the procedure in [52, 57] only applies to cw-conditions while in our experiment there is a fast dynamical variation of the current between two different values. In this way the relation $\gamma_a = \gamma_a(I_{\text{on}})$ shown in Fig. 3(b) represents an effective value of γ_a due to the modulated operation of the device.

We show in Fig. 4(a) the time evolution of the power of the two linearly polarized modes obtained with the same modulation conditions that were considered in the experimental results of Fig. 2 and Fig. 3. A good agreement between our theoretical and experimental results is observed. Fig. 4(a) shows that are some pulses in which one of the polarizations dominates over the other during all its duration (see for instance the pulses beginning at 510 and 600 ns). There is also a strong competition between both polarizations in some of the pulses (see for instance the pulses beginning at 520 and 590 ns). If a much smaller modulation frequency is considered, the $x-$polarized mode always dominates at the end of all pulses because the stable solutions are reached. These solutions correspond to those observed in the cw-light current characteristics, i.e., a large and a small value of the power for the $x-$ and $y-$polarization modes, respectively. We have checked that situation in our experiments and in our numerical simulations.

The dynamical evolution of the carrier number normalized by its value at threshold is shown in Fig. 4(b). This figure shows that the number of carriers decrease below the threshold value

after the laser is switched-off (see, for instance, Fig. 4(b) for $515 < t < 520$ ns) in such a way that spontaneous emission noise dominates the evolution of both linearly polarized modes. Fluctuations due to spontaneous emission then rule which linear polarization mode will be preferably excited during the next pulse.

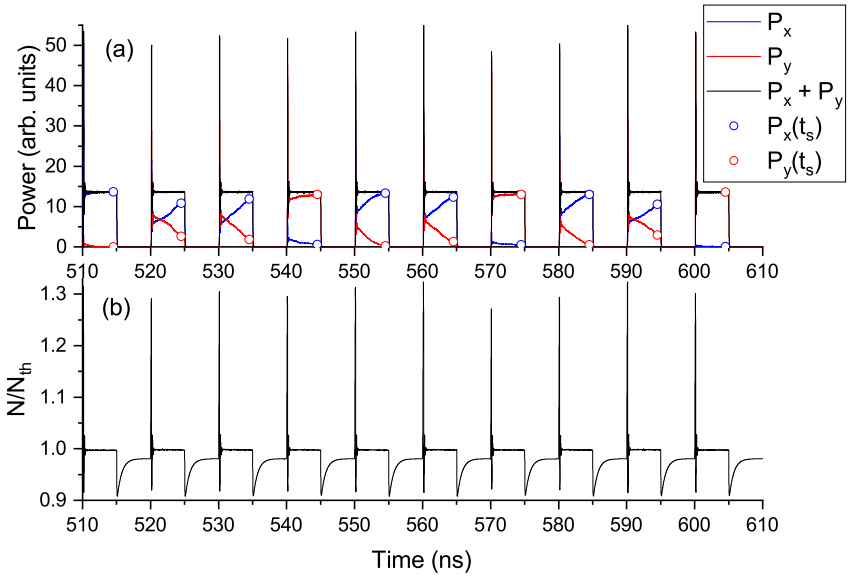

Fig. 4. (a) Simulated time traces of the power of x (blue line) and y (red line) polarization modes. The total power is also plotted with black line. (b) Simulated time traces of the ratio between the carrier number and carrier number at threshold. $f_{\mathrm{mod}} = 100$ MHz, $I_{\mathrm{on}} = 15.8$ mA ($V_{\mathrm{on}} = 1.3$ V), $I_{\mathrm{off}} = 2.5$ mA, $\gamma_a = -0.013$ ns^{-1}, and t_s=4.5 ns.

Fig. 5(a) shows the theoretical probability density function (pdf) of the $x-$ and $y-$polarized signals obtained with the modulation conditions and sampling time considered in Fig. 4. Both pdfs have local maxima that appear close to the minimum and maximum values of the signals. The corresponding experimental pdfs are shown in Fig. 5(b). Good agreement is found between the experimental and theoretical results. This agreement could be improved by including the effect of the noise in the photodetectors that has not been taking into account in our model. We have also calculated the histogram of the ratio of the two experimental signals at the sampling time, $V_y(t_s)/V_x(t_s)$. Results corresponding to the pdfs in Fig. 5(b) are shown in the new Fig. 5(c). We have considered 5000 experimental values of $V_y(t_s)/V_x(t_s)$. Fig 5(c) shows that the histogram decreases as $V_y(t_s)/V_x(t_s)$ increases. There is an accumulation of probability at low values of that ratio: 80 % of the data have $V_y(t_s)/V_x(t_s)$ between 0 and 10. In the remaining data we find situations in which $V_y(t_s)/V_x(t_s)$ reach very high values, indicating that the power of the x-polarization is still very small at the sampling time.

5. Theoretical results for a VCSEL with no anisotropies

In this section we analyze the expected results when a VCSEL with no anisotropies is considered. This can be taken into account in the theoretical model by assuming zero values for the amplitude and phase anisotropies, i. e., $\gamma_a = \gamma_p = 0$. Since we do not have a real device with such values of linear dichroism and birefringence we have to limit ourselves to a theoretical analysis. For this isotropic VCSEL the statistical properties of the light emitted in both linearly polarized modes are expected to be similar. This is illustrated in Fig. 6 where the theoretical pdfs of the power of the $x-$ and $y-$polarizations are plotted for two different sampling times. $x-$ and $y-$polarized

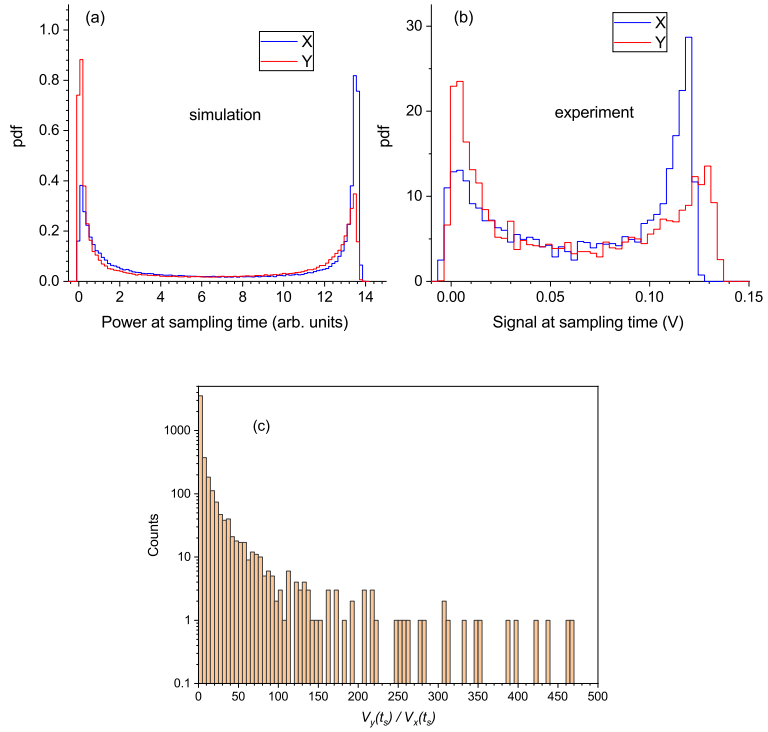

Fig. 5. (a) Theoretical and (b) experimental pdfs of x and y signals at t_s= 4.5 ns. (c) Experimental histogram of $V_y(t_s)/V_x(t_s)$. f_{mod} = 100 MHz, I_{on} = 15.8 mA (V_{on} = 1.3 V), I_{off} = 2.5 mA, $\gamma_a = -0.013$ ns^{-1}, and γ_p = 103.34 ns^{-1}.

pdfs are very similar for both sampling times. For a large value of the sampling time both pdfs have two local maxima similarly to those shown in Fig. 5(a). Those local maxima decrease as the sampling time decreases in such a way that both pdfs become nearly constant when t_s is close to the rising edge of the pulses corresponding to the total power.

Since the statistical properties of the light emitted in both linearly polarized modes are similar, we would expect that $P(X > Y)$ is independent of the value of the sampling time in isotropic VCSELs, taking a value close to 0.5. This is illustrated in Fig. 7(a) in which $P(X > Y)$ is plotted as a function of t_s for the same modulation conditions considered in Fig. 6. Each point has been calculated using a different simulation over 10^6 modulation periods. There are several advantages to using isotropic VCSELs for random number generation. The first one is that the bias of raw bits, $e = P(X > Y) - 1/2 = p(0) - 1/2$, is small. The second one is that e is independent of the sampling time, and the third one is that a small value of e is obtained independently of the modulation parameters (f_{mod}, I_{on}, and I_{off}). The first two advantages are well illustrated in Fig. 7(a). The third one will be illustrated in the following section in which we will consider much higher modulation frequencies.

The independence of the values of $P(X > Y)$ on t_s is also well illustrated when comparing with the values that are obtained with the parameters corresponding to the VCSEL described in section 2. These values are shown in Fig. 7(b): there is a monotonous increase of $P(X > Y)$ (over a much wider range than that in Fig. 7(a)) as t_s increases. A similar increase was observed in previous experiments under the same experimental conditions [46].

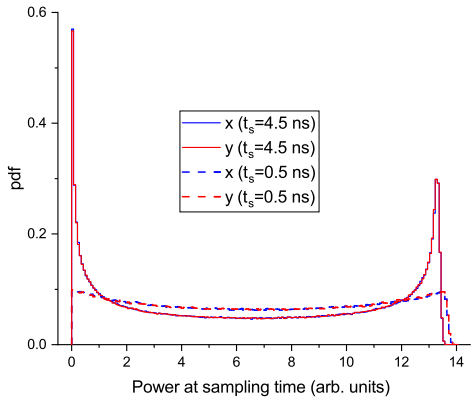

Fig. 6. Theoretical pdfs of $x-$ and $y-$power at two sampling times, t_s=0.5 ns, and t_s=4.5 ns. f_{mod} = 100 MHz, I_{on} = 15.8 mA, $I_{\text{off}} = 2.5mA$, $\gamma_a = 0$ ns^{-1}, $\gamma_p = 0$ ns^{-1}.

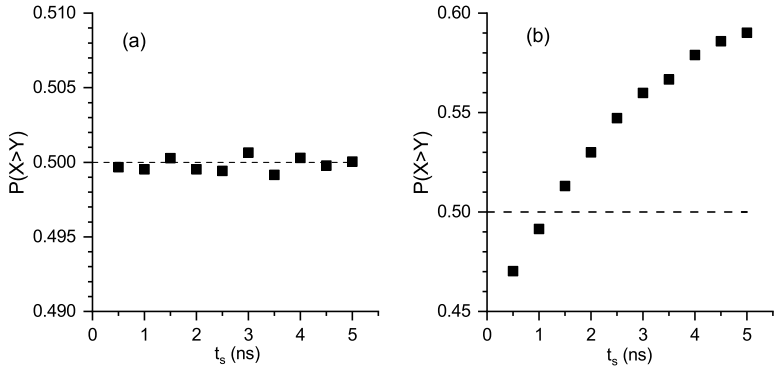

Fig. 7. Probability of excitation of the $x-$polarization as a function of the sampling time for (a) $\gamma_a = 0$ ns^{-1}, $\gamma_p = 0$ ns^{-1}, and (b) $\gamma_a = -0.013$ ns^{-1}, $\gamma_p = 103.34$ ns^{-1}. f_{mod} = 100 MHz, I_{on} = 15.8 mA, $I_{\text{off}} = 2.5mA$.

6. Quantum random number generation at high modulation frequencies

In this section we analyze the random number generation process using a VCSEL that is gain-switched at a repetition frequency of 2 GHz, much larger than in previous sections. We can only present theoretical results, as the 600 MHz bandwidth limitation of our laser mount prevents us from achieving high modulation frequencies. We will present results obtained with i) the parameters of the VCSEL that we have used in the experiments, ii) the parameters of the isotropic VCSEL, and iii) another set of parameters that will help us to understand the evolution of the probability of excitation of a given linear polarization.

6.1. Theoretical results at high modulation frequencies

Fig. 8(a) shows the time evolution of the power of the two linearly polarized modes of the VCSEL described in section 2 and section 3 when f_{mod} = 2 GHz, I_{on} = 15.8 mA, and I_{off} = 0 mA. While the value of I_{on} is equal to that considered in previous figures, the value of I_{off} has been decreased to zero for randomizing the evolution of both linear polarizations before the next pulse is emitted :

if the value of I_{off} chosen at f_{mod}=100 MHz, 2.5 mA, is maintained at f_{mod}=2 GHz, the decrease of the carrier number during the switch-off part of the modulation period is not enough for the power of both linear polarizations to reach the small values dominated by spontaneous emission noise. It is necessary to significantly decrease the value of I_{off} for having a fast decrease of the carrier number (see Fig. 8(b) from t =30.25 ns to t =30.5 ns) that leads to the noisy values of P_x and P_y observed in Fig. 8(a) at the end of the modulation period (t =30.5 ns). The vertical scale is logarithmic in order to appreciate better the fluctuations induced by the spontaneous emission noise. The total power is also included in the figure. Similarly to low modulation frequency results, random excitation of linear polarizations is observed in Fig. 8(a) due to the decrease in the number of carriers well below the threshold value (shown in Fig. 8(b)) which leads to spontaneous emission events dominating the dynamical evolution.

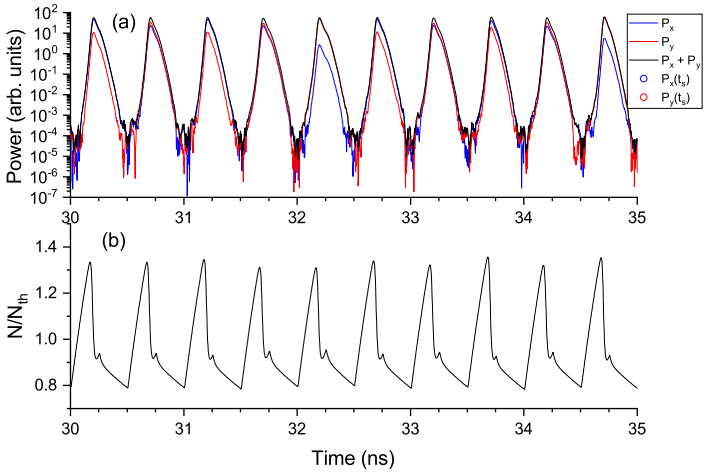

Fig. 8. (a) Simulated time traces of the power of x (blue line) and y (red line) polarization modes. The total power is also plotted with black line. (b) Simulated time traces of the ratio between the carrier number and carrier number at threshold. f_{mod} = 2 GHz, I_{on} = 15.8 mA, I_{off} = 0 mA, $\gamma_a = -0.013$ ns^{-1}, and $\gamma_p = 103.34$ ns^{-1}.

An analysis, similar to that reported in Fig. 7, on the dependence of $P(X > Y)$ on the sampling time is shown in Fig. 9(a). This figure shows that $P(X > Y)$ has a minimum at a value of the sampling time $t_s = 0.2$ ns for the VCSEL considered in our experiments ($\gamma_p = 103.34$ ns^{-1}). This value is very close to the time at which the total power has a maximum, as can be seen in Fig. 8(a). Results corresponding to the isotropic VCSEL are also included in Fig. 9(a). Similarly to Fig. 7(a), $P(X > Y)$ is independent of t_s and with a value close to 0.5.

Results corresponding to the VCSEL of our experiments excited with a larger value of I_{on} are shown in Fig. 9(b) with squares. Again a minimum $P(X > Y)$ appears at a value close to the time at which the total power develops a maximum. This time is smaller than that in Fig. 9(a) because the value of I_{on} is larger in Fig. 9(b). The values of $P(X > Y)$ are larger in Fig. 9(b) than in Fig. 9(a) since increasing the values of I_{on} favours the $x-$polarization.

Fig. 9 shows that $P(X > Y)$ is smaller than 0.5 when simulations are performed using the parameters of our VCSEL ($\gamma_p = 103.34$ ns^{-1}) modulated with $f_{mod} = 2$ GHz and for two different values of I_{on}. This happens even if the amplitude anisotropy favours the $x-$polarization. This polarization is favoured because the γ_a values (see Fig. 3(b)) are negative for both values of I_{on}. To understand why the $x-$polarization is not preferently excited when the amplitude anisotropy favours it we have to consider the role played by the other VCSEL anisotropy, the phase anisotropy characterized by the γ_p parameter. We now analyze how the results change when changing the

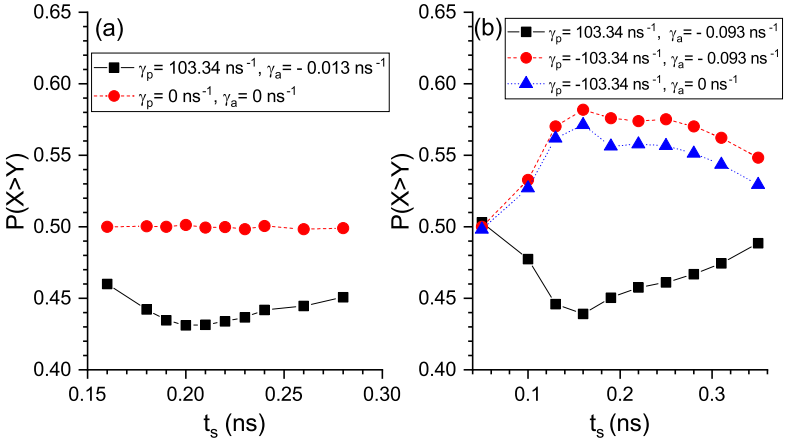

Fig. 9. Probability of excitation of the $x-$polarization as a function of the sampling time for (a) $I_{\text{on}} = 15.8$ mA, and (b) $I_{\text{on}} = 24.5$ mA. $f_{\text{mod}} = 2$ GHz, and $I_{\text{off}} = 0$ mA.

sign of γ_p. The change of this sign means that the optical frequency of the $x-$polarization is larger than that corresponding to the $y-$polarization ($\nu_x > \nu_y$). Fig. 9(b) shows with circles the effect of changing the sign of γ_p on $P(X > Y)$. $P(X > Y)$ is now always larger than 0.5. This indicates the important role also played by the phase anisotropy: the linearly polarized mode that is preferently excited is the one that has the largest value of the optical frequency. This is also confirmed by considering the case in which no amplitude anisotropies appear and only phase anisotropies are considered. This is shown in Fig. 9(b) with triangles: again the $x-$linearly polarized mode is preferently excited. The asymmetric behavior between both linearly polarized modes is caused by the frequency asymmetry induced by the linewidth enhancement factor.

6.2. Post-processing and quality of randomness

One of the usual ways to test the quality of randomness is to perform the NIST statistical test. For this, we obtained a long bit stream from the simulation of 1.413×10^9 periods similar to those shown in Fig. 8(a). The considered parameters are those corresponding to the VCSEL that we have used in our experiments with a sampling time of $t_s = 0.2$ ns. The value of the bias obtained for the complete sequence of raw bits is $e = -6.95 \times 10^{-2}$. We consider a post-processing technique using linear corrector codes [33,61]. We use the efficient $[n, k, d]$-BCH codes defined over the finite field $GF(2)$ where $n+1$ is a power of 2 [33,62]. Using appropriate values of k and n, the throughput (k/n) can be close to 1, while maintaining a very efficient bias reduction [61] and achieving practically good level of security [62]. We have used the BCH code with parameters [1023,1003,5] as in Ref. [33]. Using this post-processing we obtain a high throughput, 98%, and 1.385×10^9 bits that have a bias of -6.96×10^{-7}. Some other post-processing methods like the Toeplitz-Hash algorithm are usually considered in the literature [63]. In both algorithms, the linear corrector codes and the Toeplitz-Hash, a matrix with k rows and n columns (G and T, respectively) is used to transform n raw input bits into k post-processed bits. There are a couple of notable differences: i) T is a dense matrix and requires a random bit vector [63], and ii) G is a sparse matrix that is defined by the coefficients of a known cyclic polynomial [61]. As a consequence, a post-processing using G is more computationally efficient than using T, both hardware and software. In any case, a more exhaustive comparison between both post-processing methods is desirable to know their advantages and disadvantages. This comparison will be the subject of future work.

Figure 10 (a) shows the results obtained with the NIST statistical test applied to the post-processed bits. Each test is performed using 1000 sequences of 1 million bits each with a statistical significance level, $\alpha = 0.01$. In Fig. 10 we show the P-value$_T$, that gives an idea of the uniformity of the distribution of the P-values [49], and the proportion of sequences passing the test. For test that return multiple P-value$_T$ and proportions, the more representative case, that is the one having a P-value$_T$ closest to the median of P-value$_T$, has been plotted. Two criteria are used in these tests for "success": i) the P-value$_T$ must be larger than 10^{-4}, and ii) the proportions must be in the (0.9805607,0.9994393) confidence interval [49]. These values have been included in Fig. 10 using horizontal dashed lines. Results shown in Fig. 10 (a) confirm that the post-processed bits sequences obtained from the simulation of the VCSEL's dynamics at 2 Gbps rate are sufficiently random for passing the statistical test of NIST.

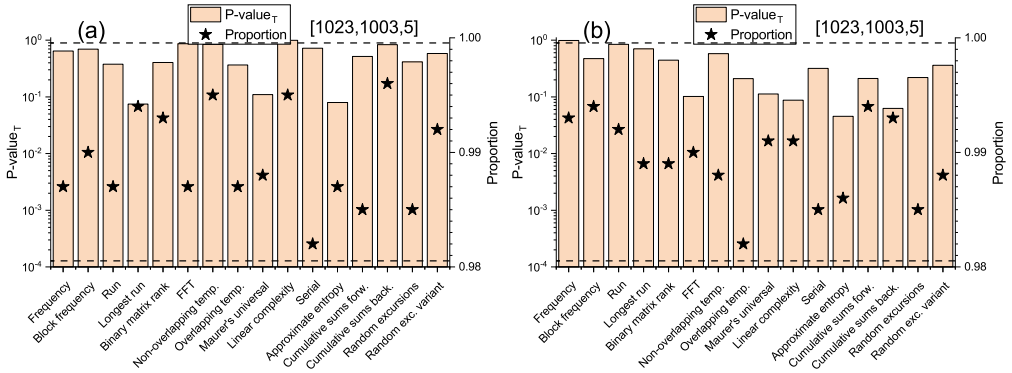

Fig. 10. NIST test results for data obtained using (a) the parameters of the VCSEL of our experiment ($\gamma_a = -0.013$ ns^{-1}, and $\gamma_p = 103.34$ ns^{-1}), and (b) the parameters of the isotropic VCSEL ($\gamma_a = \gamma_p = 0$ ns^{-1}). $f_{\text{mod}} = 2$ GHz, $I_{\text{on}} = 15.8$ mA, $I_{\text{off}} = 0$ mA, and $t_s = 0.2$ ns.

We perform a similar analysis for the case of the isotropic VCSEL by using the same simulation parameters with the exception of γ_a and γ_p ($\gamma_a = \gamma_p = 0$ ns^{-1}). The value of the bias obtained for the complete sequence of raw bits, 1.130×10^9 bits, is $e = -9.76 \times 10^{-4}$. We now wonder if this raw data bits pass the statistical test, so we have used them as input for the NIST statistical test suite with $\alpha = 0.01$. We have tested the randomness of 1000 sequences of 1 million bits each. There are 10 tests for which the proportion of sequences that pass the tests is larger than 98% (block frequency, longest runs, binary matrix rank, FFT, non-overlapping template, Maurer's universal, linear complexity, entropy, random excursions and random excursions variant). The proportion obtained for the other six test does not reach the 98% value, going from 69% (frequency test) to 97.2% (serial test). In this way these raw data bits do not pass NIST test. These results remark the necessity of a post-processing of the raw data in order to pass the complete set of NIST tests. In this way we have used the same [1023,1003,5]-BCH code to obtain 1.108×10^9 bits that have a bias of -2.21×10^{-5}. Figure 10 (b) shows the results obtained with the NIST statistical test applied to these post-processed bits. These results confirm that the post-processed bits sequences obtained for the isotropic VCSEL at 2 Gbps rate are also sufficiently random for passing the statistical test of NIST.

The P-value$_T$ and the proportions averaged over the 16 tests, <P-value$_T$> and <Prop>, can be used to quantitatively summarize the results of the test of NIST [33]. The spreading of proportions around <Prop> is also quantified by including the standard deviation of the proportions over the tests, σ_{Prop}. The values of these quantities for Fig. 10(a) (Fig. 10(b)) are <P-value$_T$>=0.5326 (0.3600), <Prop>=0.9894 (0.9894) and σ_{Prop}=0.0043 (0.0036). These values are similar to those

experimentally obtained at much smaller modulation frequencies [33].

7. Summary and Conclusion

Summarizing, we have reported a characterization of the fluctuations of the linearly polarized modes of a gain-switched VCSEL for QRNG applications. We have compared our experimental results with those obtained from a stochastic rate equations model incorporating the intrinsic parameters of the laser found using the state-of-the-art experimental techniques. We have found good agreement between our experiments and simulations only when considering the dependence of the linear dichroism of the VCSEL on the injected bias current. This good agreement can be used to establish a validation process that permits to monitor the device behaviour to detect malicious intrusion or malfunctioning of the QRNG. For instance, we can consider a laser-seeding attack on the QRNG similar to that analyzed for QKD [64]. This attack consists of an eavesdropper injecting light into the VCSEL to try to change the light emitted by the device in such a way that the sequence of random bits is determined by that eavesdropper. This attack can be detected when comparing the theoretical and experimental pdfs shown in Fig. 5 since the optical injection will change qualitatively and quantitatively the shape of the experimental pdfs. A potential countermeasure would be to increase the level of optical isolation of the VCSEL.

Simulations of the model have been used to look for parameters that maximize the QRNG performance. Following this direction we have considered the performance when considering a VCSEL with vanishing values of the amplitude and phase anisotropies. Using these VCSELs have the advantages of i) obtaining a low value of the bias of the raw bits, and ii) this bias is independent on the sampling time and on the modulation parameters. We have also used the simulations of the model to predict the QRNG performance at high modulation frequencies. We have demonstrated that the linear dichroism parameter is not the only relevant parameter for determining the probability of excitation of a given linearly polarized mode because the phase anisotropy can also play a key role in that determination. Finally, we have shown that random bits obtained at 2 Gbps rates, after appropriate post-processing, fully pass the NIST statistical test.

Funding Ministerio de Ciencia e Innovación. PID2021-12345OB-C22 MCIN /AEI /10.13039/ 501100011033/FEDER,UE. J. G. is partially supported by grant PID2019-110633GB-I00 funded by MCIN/AEI/10.13039/ 501100011033.

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. F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, "Secure quantum key distribution with realistic devices," Rev. Mod. Phys. **92**, 025002 (2020).
2. 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. p. 2100062 (2021).
3. M. Stipčević and Ç. K. Koç, "True random number generators," in *Open Problems in Mathematics and Computational Science,* (Springer, 2014), pp. 275–315.
4. X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, "Quantum random number generation," npj Quantum Inf. **2**, 1–9 (2016).
5. M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum random number generators," Rev. Mod. Phys. **89**, 015004 (2017).
6. 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).
7. O. Alkhazragi, H. Lu, W. Yan, N. Almaymoni, T.-Y. Park, Y. Wang, T. K. Ng, and B. S. Ooi, "Semiconductor emitters in entropy sources for quantum random number generation," Ann. der Physik p. 2300289.
8. C. Kollmitzer, S. Petscharnig, M. Suda, and M. Mehic, *Quantum random number generation* (Springer, 2020).

9. W. Luo, L. Cao, Y. Shi, L. Wan, H. Zhang, S. Li, G. Chen, Y. Li, S. Li, Y. Wang *et al.*, "Recent progress in quantum photonic chips for quantum communication and internet," Light. Sci. & Appl. **12**, 175 (2023).
10. J. Cheng, J. Qin, S. Liang, J. Li, Z. Yan, X. Jia, and K. Peng, "Mutually testing source-device-independent quantum random number generator," Photonics Res. **10**, 646–652 (2022).
11. L. K. Shalm, Y. Zhang, J. C. Bienfang, C. Schlager, M. J. Stevens, M. D. Mazurek, C. Abellán, W. Amaya, M. W. Mitchell, M. A. Alhejji *et al.*, "Device-independent randomness expansion with entangled photons," Nat. Phys. **17**, 452–456 (2021).
12. W.-B. Liu, Y.-S. Lu, Y. Fu, S.-C. Huang, Z.-J. Yin, K. Jiang, H.-L. Yin, and Z.-B. Chen, "Source-independent quantum random number generator against tailored detector blinding attacks," Opt. Express **31**, 11292–11307 (2023).
13. T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, "A fast and compact quantum random number generator," Rev. Sci. Instruments **71**, 1675–1680 (2000).
14. M. Stipčević and B. M. Rogina, "Quantum random number generator based on photonic emission in semiconductors," Rev. scientific instruments **78**, 045104 (2007).
15. W. Wei and H. Guo, "Bias-free true random-number generator," Opt. letters **34**, 1876–1878 (2009).
16. H. Fürst, H. Weier, S. Nauerth, D. G. Marangon, C. Kurtsiefer, and H. Weinfurter, "High speed optical quantum random number generation," Opt. express **18**, 13029–13037 (2010).
17. 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**, 022339 (2013).
18. 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**, 051137 (2010).
19. 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**, 063814 (2010).
20. 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. letters **35**, 312–314 (2010).
21. 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**, 20665–20672 (2011).
22. 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. Light. Technol. **30**, 1329–1334 (2012).
23. 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**, 12366–12377 (2012).
24. 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**, 1645–1654 (2014).
25. 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**, 261112 (2014).
26. Y.-Q. Nie, L. Huang, Y. Liu, F. Payne, J. Zhang, and J.-W. Pan, "The generation of 68 gbps quantum random number by measuring laser phase fluctuations," Rev. Sci. Instruments **86**, 063105 (2015).
27. C. Abellan, W. Amaya, D. Domenech, P. Muñoz, J. Capmany, S. Longhi, M. W. Mitchell, and V. Pruneri, "Quantum entropy source on an inp photonic integrated circuit for random number generation," Optica **3**, 989–994 (2016).
28. 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. Light. Technol. **36**, 3778–3784 (2018).
29. 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**, 055022 (2020).
30. 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**, 6209–6224 (2020).
31. 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**, 1–7 (2021).
32. 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**, 054012 (2021).
33. M. Valle-Miñón, A. Quirce, A. Valle, and J. Gutiérrez, "Quantum random number generator based on polarization switching in gain-switched vcsels," Opt. Continuum **1**, 2156–2166 (2022).
34. A. Alarcón, J. Argillander, D. Spegel-Lexne, and G. Xavier, "Dynamic generation of photonic spatial quantum states with an all-fiber platform," Opt. Express **31**, 10673–10683 (2023).
35. D. Hurley-Smith and J. Hernandez-Castro, "Quantum leap and crash: Searching and finding bias in quantum random number generators," ACM Trans. on Priv. Secur. (TOPS) **23**, 1–25 (2020).
36. D. Cirauqui, M. Á. García-March, G. G. Corominas, T. Graß, P. R. Grzybowski, G. Muñoz-Gil, J. Saavedra, and M. Lewenstein, "Quantum random number generators: Benchmarking and challenges," arXiv preprint arXiv:2206.05328 (2022).
37. O. Guillan-Lorenzo, M. Troncoso-Costas, D. Alvarez-Outarelo, F. J. Diaz-Otero, and J. C. Garcia-Escartin, "Optical quantum random number generators: a comparative study," Opt. Quantum Electron. **55**, 185 (2023).
38. R. Loudon, *The quantum theory of light* (OUP Oxford, 2000).

39. R. Michalzik, *VCSELs: fundamentals, technology and applications of vertical-cavity surface-emitting lasers*, vol. 166 (Springer, 2012).
40. J. Goyvaerts, A. Grabowski, J. Gustavsson, S. Kumari, A. Stassen, R. Baets, A. Larsson, and G. Roelkens, "Enabling vcsel-on-silicon nitride photonic integrated circuits with micro-transfer-printing," Optica **8**, 1573–1580 (2021).
41. 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**, 661–666 (1995).
42. V. Chizhevsky, "Bistable vertical cavity laser with periodic pump modulation as a random bits generator," Opt. Spectrosc. **108**, 343–346 (2010).
43. V. Chizhevsky, "Fast generation of random bits based on polarization noises in a semiconductor vertical-cavity laser," Opt. Spectrosc. **111**, 689–694 (2011).
44. 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).
45. R. Shakhovoy, E. Maksimova, V. Sharoglazova, M. Puplauskis, and Y. Kurochkin, "Fast and compact vcsel-based quantum random number generator," J. Physics: Conf. Ser. **1984**, 012005 (2021).
46. A. Quirce and A. Valle, "Random polarization switching in gain-switched vcsels for quantum random number generation," Opt. Express **30**, 10513–10527 (2022).
47. R. Shakhovoy and E. Maksimova, "Gain-switched vcsel as a quantum entropy source: the problem of quantum and classical noise," St. Petersburg Polythechnic Univ. Journal: Phys. Math. **15**, 201–205 (2022).
48. I. Rivero, A. Lazaro del Pozo, M. Valle-Miñon, A. Quirce, and A. Valle, "Measurement of the temperature dependence of polarization switching in gain-switched vcsels for quantum random number generation," Photonics **10**, 474 (2023).
49. A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert *et al.*, "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 Publ. **800**, 22 (2010).
50. A. Quirce and A. Valle, "Phase diffusion in gain-switched semiconductor lasers for quantum random number generation," Opt. Express (2021).
51. P. Pérez, A. Valle, I. Noriega, and L. Pesquera, "Measurement of the intrinsic parameters of single-mode vcsels," J. Light. Technol. **32**, 1601–1607 (2014).
52. P. Pérez, A. Valle, and L. Pesquera, "Polarization-resolved characterization of long-wavelength vertical-cavity surface-emitting laser parameters," J. Opt. Soc. Amer. B **31**, 2574–2580 (2014).
53. A. Quirce, C. de Dios, A. Valle, L. Pesquera, and P. Acedo, "Polarization dynamics in vcsel-based gain switching optical frequency combs," J. Light. Technol. **36**, 1798–1806 (2018).
54. A. Valle, M. Sciamanna, and K. Panajotov, "Irregular pulsating polarization dynamics in gain-switched vertical-cavity surface-emitting lasers," IEEE J. Quantum Electron. **44**, 136–143 (2008).
55. J. Martin-Regalado, F. Prati, M. San Miguel, and N. Abraham, "Polarization properties of vertical-cavity surface-emitting lasers," IEEE J. Quantum Electron. **33**, 765–783 (1997).
56. 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**, 1–9 (2019).
57. M. Van Exter, M. Willemsen, and J. Woerdman, "Polarization fluctuations in vertical-cavity semiconductor lasers," Phys. Rev. A **58**, 4191 (1998).
58. 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**, 636–642 (2015).
59. H. Risken, "Fokker-planck equation," in *The Fokker-Planck Equation,* (Springer, 1996).
60. P. E. Kloeden and E. Platen, "Stochastic differential equations," in *Numerical Solution of Stochastic Differential Equations,* (Springer, 1992).
61. P. Lacharme, "Post-processing functions for a biased physical random number generator," in *International Workshop on Fast Software Encryption,* (Springer, 2008), pp. 334–342.
62. 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.
63. X. Ma, F. Xu, H. Xu, X. Tan, B. Qi, and H.-K. Lo, "Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction," Phys. Rev. A **87**, 062327 (2013).
64. V. Lovic, D. G. Marangon, P. Smith, R. I. Woodward, A. J. Shields *et al.*, "Quantified effects of the laser-seeding attack in quantum key distribution," Phys. Rev. Appl. **20** (2023).