
Article:
Lovic, V, Marangon, Davide Giacomo, Lucamarini, Marco orcid.org/0000-0002-7351-4622 et al. (2 more authors) (2021) Characterizing Phase Noise in a Gain-Switched Laser Diode for Quantum Random-Number Generation. Physical Review Applied. 054012. ISSN 2331-7019

https://doi.org/10.1103/PhysRevApplied.16.054012

Characterizing Phase Noise in a Gain-Switched Laser Diode for Quantum Random-Number Generation

V. Lovic,[1,2] D.G. Marangon,[1,*] M. Lucamarini,[1] Z. Yuan,[1] and A.J. Shields[1]

[1] *Toshiba Europe, Ltd., 208 Cambridge Science Park, Milton Road, Cambridge CB4 0GZ, United Kingdom*

[2] *QOLS, Blackett Laboratory, Imperial College London, South Kensington, London SW7 2AZ, United Kingdom*

(Received 11 June 2021; revised 12 August 2021; accepted 1 October 2021; published 4 November 2021)

While operating a quantum random-number generator (QRNG), it is extremely useful to have a model of the physical entropy source to guarantee that the device is delivering randomness of genuine quantum origin. In this work we consider a QRNG based on a gain-switched laser diode and we develop a model to quantify its phase noise. This model is based on the laser rate equations and the state-of-the-art techniques for the characterization of laser diodes used in lightwave systems. These tools let us achieve a faithful modeling of the phase noise and we verify its accuracy through comparisons with experimental measurements. Furthermore, the model can be used to select optimal parameters to maximize the QRNG performance and monitor the device behavior to detect malfunctioning or malicious tampering of the device.

DOI: 10.1103/PhysRevApplied.16.054012

I. INTRODUCTION

Unpredictability is an essential resource for cryptographic applications, both classical and quantum. In the last few years, many schemes to generate random numbers out of processes of quantum origin have been devised, boosted by the promise of ultimate unpredictability [1,2]. However, in order to guarantee unpredictability, the scheme has to be rigorously implemented within the boundaries drawn by a theoretical model of the employed quantum process. This is especially true for the so-called device-dependent quantum random-number generators (QRNGs) whose notion of security strongly depends on assumptions that have to be defined and hold for both the parts of quantum state preparation and measurement. In contrast, the class of semidevice-independent and device-independent QRNGs allow the user to relax the assumptions on either one or both the parts, respectively, but this typically comes at the cost of a lower final secure generation rate [3–5].

Recently, many different device-dependent generation schemes have been introduced based on measuring laser phase noise, which is a source of quantum randomness resulting from spontaneous emission [6–8]. Using an asymmetric interferometer, laser phase noise can be converted to random fluctuations of intensity at the interferometer output, which can be measured and digitized. All the recent implementations of the scheme achieved ultrafast generation rates, in the order of hundreds of Mbps and Gbps [7,9], by employing gain-switched laser diodes (LDs) commonly used in ligthwave communication systems.

In this work, we develop a general model that can be applied to phase-noise QRNGs using gain-switched LDs. First, we implement state-of-the-art techniques from the field of fiber-optic communications to calibrate the parameters in our model based on experimental measurements. For engineering high-end telecommunication devices, it is essential to predict what the diode performances will be with different modulation regimes and a vast literature indeed exists on the subject of LD modeling and characterization [10–14]. With these analytical and numerical tools we build a model that can be used to identify the operational limits within which LDs should be operated for random-number generation. In terms of the device-dependent framework this is essential because unpredictability can only be achieved when the laser is driven in such a way that spontaneous emission becomes the dominant process between two gain-switched pulses. Second, we develop simple method for measuring phase noise in gain-switched LDs. This allows us to validate the operational limits established by the model by comparing measurements of the phase noise to the model predictions. The device characterization can be performed at the beginning of the operational lifetime of the device, as part of a certification process. Once the model parameters have been determined, verified, and the operational limits

*Corresponding author. davide.marangon@crl.toshiba.co.uk

established, the QRNG can be programmed to monitor certain key parameters, such as bias current, or level of phase noise, and take corrective action if these parameters fall outside the operational range established by the characterization. Furthermore, the model can be used to explore different parameters and select optimal ones to maximize performance.

In Sec. II, we briefly review random phase QRNGs and the recent literature regarding physical characterization. In Sec. III, we develop a rate-equation model for the purposes of quantifying laser phase noise. We introduce a technique to estimate the rate-equation-model parameters and we verify the model accuracy with comparisons to experiment. In Sec. IV, we use the rate equations to model the impact of the spontaneous emissions on the laser phase noise. Section V draws the connection between laser phase noise and the effects this has on the performance of the QRNG. We discuss our results in Sec. VI and conclude in Sec. VII.

II. LASER PHASE NOISE

Laser phase noise is a consequence of spontaneous emission [15–17]. Each spontaneously emitted photon has a random phase that is added to the total electromagnetic field, leading to random phase fluctuations. These fluctuations can be measured using an asymmetric interferometer to interfere the laser output with a delayed version of itself, as in Fig. 1. During this time delay, spontaneous emission events in the laser cavity randomize the phase, leading to the interference of light with a random phase difference at the interferometer output. This converts the random phase into a random intensity, which can be measured and digitized to generate random numbers. The intensity at the output of the asymmetric interferometer is given by

$$I_{\text{out}} = \frac{I_{\text{in}}}{2}[1 + \cos(\Delta\phi + \phi_0)], \tag{1}$$

where I_{in} is the input intensity, $\Delta\phi$ is the random phase difference between delayed and nondelayed light due to spontaneous emission, and ϕ_0 is the relative phase between both interferometer arms due to the difference in their length. A key assumption made in phase-noise QRNGs is that spontaneous emission fully randomizes the phase during the time delay of the asymmetric interferometer. That is, the phase difference $\Delta\phi$ between the light that has passed through the short and long arms of the interferometer is uniformly distributed in the interval $[-\pi, \pi)$. I_{out} would then follow an arcsine distribution. In reality, the phase is a Gaussian random variable [15], but a Gaussian distribution with a large variance, wrapped over the interval $[-\pi, \pi)$, is a good approximation to a uniform distribution. Still, it is useful to quantify the phase noise, i.e., the variance of the Gaussian phase distribution, to ensure the variance is large enough for this approximation to hold.

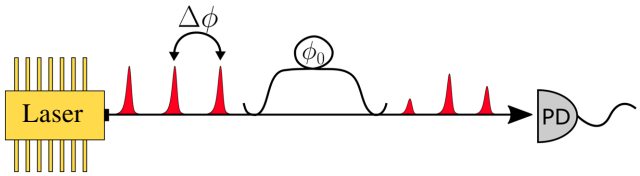

FIG. 1. A typical phase noise QRNG setup. During the time delay of the interferometer, spontaneous emission in the laser cavity randomizes the phase, leading to random intensities at the interferometer output.

For a cw operated laser, as used in demonstrations of phase-noise QRNGs [18,19], quantifying the phase noise is straightforward: the variance of the Gaussian phase distribution is inversely proportional to the coherence time (τ_c) of the laser

$$\langle \Delta\phi^2(t) \rangle = \frac{2t}{\tau_c}. \tag{2}$$

Therefore, in order guarantee an approximately uniform phase distribution, the time delay of the interferometer must be much longer than the coherence time, which limits the sampling rate and hence the performance of the QRNG. To increase phase noise, the laser can be gain switched [6–8]. By driving the laser below threshold between measurements, the phase noise is drastically increased, enabling state-of-the-art RNG rates with little added complexity. However, quantifying the phase noise in a gain-switched laser is more challenging. Equation (2) no longer applies since the laser linewidth, and hence coherence time, strongly depends on the current. Previous works have attempted to address this challenge in the context of QRNG, and also quantum key distribution (QKD) where phase randomized pulses of light are also required. The use of gain switching to maximize laser phase noise for QRNG was pioneered by Jofre *et al.* [6]. In Ref. [7] the authors use a rate-equation model to estimate the phase noise. The model parameters were a combination of typical parameters for semiconductor lasers, not specific to their own laser, and parameters that were selected to best fit the observed gain-switched power output of the laser. They quantify the phase noise using the following linear approximation [16]:

$$\langle \Delta\phi^2(t) \rangle = \frac{R}{2S}(1 + \alpha^2)t, \tag{3}$$

where R is the rate of spontaneous emission, S is the number of photons, and α is the linewidth enhancement factor (also known as the Henry factor). R and S can be obtained from the solution of the rate equations, and hence Eq. (3) can be used to calculate the phase noise for any given current input.

Reference [20] presents a method of measuring phase randomness by observing the visibility of interference between successive pulses from a gain-switched laser. This technique was used to verify that a gain-switched laser diode can be operated at 10 GHz with sufficient phase randomization for the secure implementation of QKD protocols.

Another rate-equation-based approach is presented in Ref. [21]. The authors implement a stochastic rate-equation model to analyze the phase noise. They use the Monte Carlo method to estimate the variance of the phase due to phase noise. This approach has the advantage of not relying on linear approximations such as Eq. (3) and accounting for nonlinear effects, such as relaxation oscillations, which are significant for gain-switched lasers.

In this work we build upon previous results [7,20,21] and develop a stochastic rate-equation model to quantify laser phase noise. We provide two main improvements: first, we implement established techniques from the field of classical fiber-optic communications to extract the rate-equation-model parameters for our specific laser. Second, we develop a simple method for measuring laser phase noise in a gain-switched laser. Together, these improvements allow us to make accurate quantitative simulations of the laser power output and phase noise, and to verify the accuracy of these simulations with comparisons to experimental measurements. This work therefore presents a complete picture, from modeling to calibration measurements and experimental verification of the model.

III. RATE-EQUATION MODEL

Laser rate equations are a very well-established method for modeling semiconductor laser dynamics [10,11]. They are widely used for simulating fiber-optic communication system performance, where semiconductor lasers are used extensively [13]. We take advantage of the advanced development of this technique to build a rate-equation model for the purpose of modeling laser phase noise and quantifying the quantum randomness produced in a phase-noise QRNG. We verify the accuracy of our model through comparisons with experimental measurements.

The laser rate equations are a system of three coupled differential equations describing the interactions between the carrier density N, photon density S, and phase ϕ of the laser. The single-mode rate equations are

$$\frac{dN(t)}{dt} = \frac{I(t)}{qV} - \frac{N(t)}{\tau_n} - g\frac{N(t)-N_0}{1+\varepsilon S(t)}S(t), \tag{4}$$

$$\frac{dS(t)}{dt} = \Gamma_a g\frac{N(t)-N_0}{1+\varepsilon S(t)}S(t) - \frac{S(t)}{\tau_p} + \frac{\Gamma_a \beta N(t)}{\tau_n}, \tag{5}$$

$$\frac{d\phi(t)}{dt} = \frac{\alpha}{2}\left[\Gamma_a g[N(t)-N_0] - \frac{1}{\tau_p}\right], \tag{6}$$

and the power output of the laser is related to the photon density by

$$P(t) = \frac{V\eta h\nu}{2\Gamma_a \tau_p}S(t). \tag{7}$$

The rate-equation parameters are as follows: $I(t)$ is the injection current, V is the volume of the active gain medium, q is the electron charge, τ_n is the carrier lifetime, τ_p is the photon lifetime, g is the differential gain coefficient, ε is the gain compression factor, N_0 is the number of carriers at transparency, β is the fraction of spontaneous emission coupled into the lasing mode, Γ_a is the mode confinement factor, α is the linewidth enhancement factor, η is the differential quantum efficiency, ν is the frequency, and h is Planck's constant. By numerically solving the rate equations for a given current input we can obtain estimates of the power and phase of the laser output. Note that Eq. (6) describes the deterministic evolution of phase due to changes in the refractive index of the lasing medium that occur with changes in the carrier density. In the following we are not concerned with this deterministic evolution of the phase, but rather with the random fluctuations of phase driven by spontaneous emission in the laser cavity. To model the effects of spontaneous emission, a set of Langevin noise terms can be added to the rate equations [22,23]:

$$F_N(t) = F_Z(t) - \frac{F_S(t)}{\Gamma_a}, \tag{8}$$

$$F_S(t) = \sqrt{\frac{2\Gamma_a \beta N(t)S(t)}{\tau_n \Delta t}} \times x_S, \tag{9}$$

$$F_\phi(t) = \sqrt{\frac{\Gamma_a \beta N(t)}{2\tau_n S(t)\Delta t}} \times x_\phi, \tag{10}$$

where $F_Z(t) = \sqrt{2N(t)/(V\tau_n\Delta t)} \times x_Z$ is a Langevin noise term, uncorrelated to $F_S(t)$ and $F_\phi(t)$, used to define the carrier-density noise term $F_N(t)$. Δt is the time step of the integration and $x_{S,\phi,Z}$ are three independent random numbers taken from a Gaussian distribution with zero mean and unit variance. The terms $F_N(t), F_S(t)$, and $F_\phi(t)$ are added to the rate Eqs. (4)–(6), respectively. An analytical expression for the phase-noise variance $\langle \Delta\phi^2(t) \rangle$, which is valid for large signal modulations cannot be obtained. Instead, the phase-noise variance can be estimated using the Monte Carlo approach [21]. The stochastic rate equations can be

solved repeatedly and each solution will yield a different, random value for $\Delta\phi$, according to the underlying Gaussian phase distribution. The variance of these solutions for $\Delta\phi$ therefore gives an estimate of $\langle\Delta\phi^2(t)\rangle$.

Each laser has a unique set of rate-equation parameters. Therefore, to quantitatively model the behavior of a specific laser it is necessary to extract these parameters based on measurements of the laser. In the following section we implement a parameter extraction method based on simple measurements of three quantities [24–26]: the laser intensity modulation (IM) response, the transfer function of a dispersive optical fiber, and the power-current (PI) curve of the laser. Analytical expressions for these quantities can be derived from the rate equations, thereby relating the rate-equation parameters to experimentally observable quantities. By fitting these measurements to their analytical expressions, we can estimate all the rate-equation parameters. These three measurements are selected for being simple to implement using standard fiber-optic laboratory equipment, while fully constraining the rate-equation parameters.

A. Experimental validation

Our experimental setup is shown in Fig. 2 and consists of a 13.5-GHz network analyzer, dc current source, laser diode, 10-GHz photodiode, and 50 km of standard single-mode optical fiber. The exact length of fiber varies according to the bandwidth of the network analyzer, and the properties of the laser, as explained below. The current source is used to set the bias current of the laser. A bias tee is used to superimpose a small modulation current from port 1 of the NA onto the dc bias current. Finally, the laser output is measured by the photodiode connected to port 2 of the network analyzer (NA). The NA is set to measure the S_{21} parameter. The 50 km of optical fiber are inserted between the laser and detector for the fiber transfer function measurement. The PI curve of the laser is separately measured using the current source, laser, and a power meter.

In the following, we describe each measurement in turn along with the analytical equations, derived from the rate equations, used to fit the measurements. These equations are standard results from semiconductor laser theory and are stated without derivation. To verify the validity of the rate-equation model and extracted parameters, we compare the model predictions of the power output of a gain-switched laser to experimental measurements.

1. Laser intensity modulation response

The laser IM response (H_{IM}) is the transfer function from current modulation to power output of the laser [10]. An analytical expression can be derived from the rate equations by modulating the current $I(t)$ and determining the leading-order approximation of the solution [27]. It is

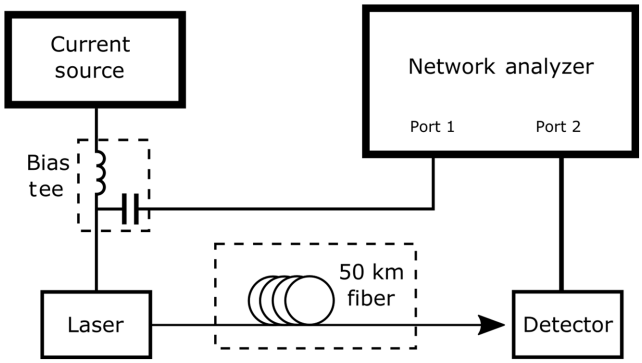

FIG. 2. Setup for measuring the laser IM response (without the fiber) and the transfer function of 50 km of dispersive fiber. Port 1 of the network analyzer sends a small modulation signal to the laser, and port 2 measures the response at the detector. The current source sets the bias current of the laser.

given by [28]

$$H_{\mathrm{IM}}(f_r) = \frac{Z}{(i2\pi f_r)^2 + i2\pi f_r\Gamma + Z}, \tag{11}$$

where $Z = 4\pi^2 {f_r}^2 + \Gamma^2/2$. Γ and f_r are the relaxation oscillation frequency and damping factor, respectively. Both quantities increase with bias current:

$${f_r}^2 = \frac{\Gamma_a g}{4\pi^2 q V}\left(I_{\mathrm{bias}} - I_{\mathrm{th}}\right), \tag{12}$$

$$\Gamma = \frac{1}{\tau_n} + K{f_r}^2, \tag{13}$$

$$K = 4\pi^2\left(\tau_p + \frac{\varepsilon}{g}\right), \tag{14}$$

where I_{bias} and I_{th} are the laser bias and threshold currents, respectively, and K is known as the K factor [29]. Experimentally, the IM response can be measured using a network analyzer [30], with one port modulating the laser, and a second port measuring the response from a detector, as shown in Fig. 2.

By measuring the IM response at different bias currents, we can determine g, τ_n, and K. The measured response will, however, contain parasitic contributions from the mount and packaging of the laser, as well as the detector. To remove the nonlaser contributions, the IM response is measured at two different bias currents, one near and one well above threshold, and the results are subtracted (in dB). The analytical expression for the subtracted IM response is therefore

$$S(f_r) = 20\log_{10}\left|\frac{H_{\mathrm{IM}}(f_r;\Gamma_1,Z_1)}{H_{\mathrm{IM}}(f_r;\Gamma_0,Z_0)}\right|, \tag{15}$$

where the subscript 0 (1) refers to the near (well above) threshold measurement. By fitting experimental measurements of the (subtracted) IM response to Eq. (15) we can

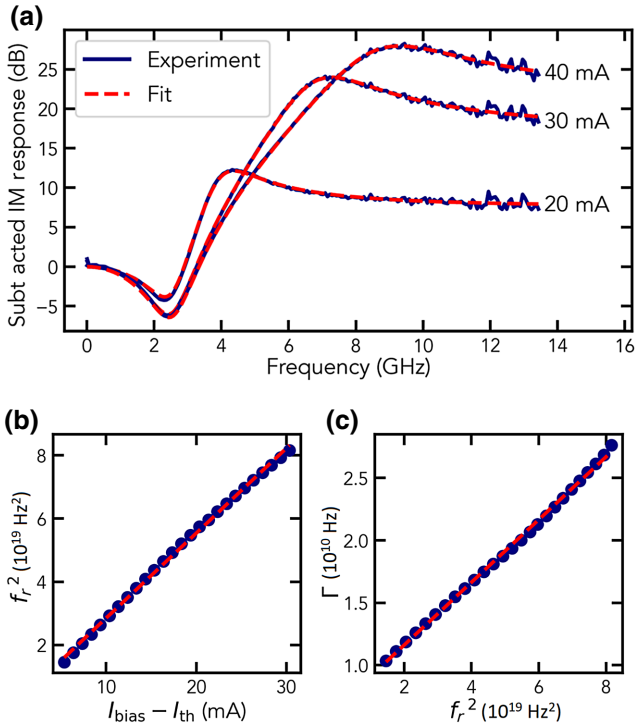

FIG. 3. (Top) The laser IM response is fitted to Eq. (15) to obtain estimates for Γ and f_r at different bias currents. (Bottom) Using the fitted Γ and f_r values we can plot Eqs. (12) and (13). Linear fits give estimates for g, τ_n, and the K factor.

estimate Γ and f_r at different bias currents [see Fig. 3(a)]. g can be determined from the gradient of a plot of f_r^2 against $I_{\text{bias}} - I_{\text{th}}$ [Fig. 3(b)] and τ_n and the K factor are determined from the intercept and gradient, respectively, of a plot of Γ against f_r^2 [Fig. 3(c)]. Our results are shown in Fig. 3, giving values of $g = 1.70 \times 10^{-6}$ cm^3/ s, $\tau_n = 0.15$ ns, and $K = 2.51 \times 10^{-10}$ s.

2. Fiber transfer function

The optical spectrum of a directly modulated laser contains modulation sidebands, which travel at different velocities through dispersive optical fiber. After a certain distance these sidebands will interfere destructively, leading to a sharp dip in the fiber transfer function [31]. An analytical expression for the fiber transfer function, using a directly modulated laser, was derived in Ref. [32] and is given by [33]

$$H_{\text{fiber}}(f) = \cos(\theta) - (\alpha - j\alpha f_c/f)\sin(\theta), \tag{16}$$

where $\theta = f^2\pi\lambda^2 DL/c$ and $f_c = \Gamma_a \varepsilon (I - I_{\text{th}})/(2\pi qV)$, D is the dispersion coefficient of the optical fiber, L is the length of the fiber, and f_c is a characteristic frequency of the laser [33,34]. The fiber transfer function can be measured using the same setup as for the laser IM response,

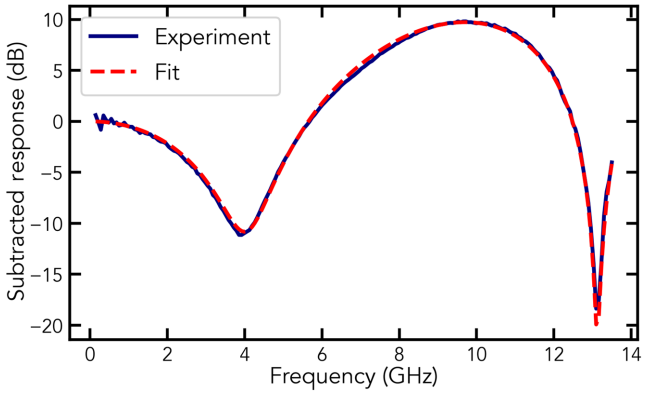

FIG. 4. The fiber transfer function is fitted to Eq. (16) to obtain estimates for α and f_c. The laser is biased at 30 mA.

and including approximately 50 km of standard single-mode fiber between the laser and detector. The fiber can be of any length, however the sharp dips in the modulation response occur at smaller frequencies for longer lengths of fiber. Given the finite bandwidth of the network analyzer (13.5 GHz in our case), a sufficiently long fiber must be used so that at least one of the dips occurs at a measurable frequency in order to properly constrain the fitting parameters. As before, by fitting the measured response to the analytical expression we can estimate α and f_c (and D, which we disregard). Again, the measured response will include contributions from the laser packaging and detector, so to remove the nonfiber contributions, the response is measured with and without the optical fiber and the results are subtracted. The fiber adds significant attenuation (approximately 10 dB) to the system, so for the measurement without the fiber we increase the attenuation using a variable optical attenuator to match the attenuation for both measurements. To account for the time delay introduced by the 50 km of fiber, the sweep time of the network analyzer needs to be reduced. The laser is biased at 30 mA. Our result is shown in Fig. 4, leading to values for $\alpha = 2.95$ and $f_c = 5.85 \times 10^8$ Hz.

3. Steady state power versus bias current

Finally, an analytical expression for the steady-state power versus bias current (PI) curve can be obtained by setting the time derivatives in the rate equations to zero. Following Ref. [24], assuming $\beta \ll 1$ and $\varepsilon/(g\tau_n) \ll 1$, the PI curve is given by

$$(FP)^2 - (I - I_{\text{th}} - I_s)FP - I_s I \approx 0, \tag{17}$$

where $F = 2e\lambda/(hc\eta)$, $I_s = \beta qV/(\Gamma_a g\tau_n\tau_p)$, and $I_{\text{th}} = qV(N_0 + 1/\Gamma_a g\tau_p)/\tau_n$. The measured PI curve can then be fitted to Eq. (17) to access these parameters. Our results are plotted in Fig. 5, giving values of $F = 4.77$ AW^{-1}, $I_s = 6.16 \times 10^{-4}$ mA, and $I_{\text{th}} = 14.7$ mA.

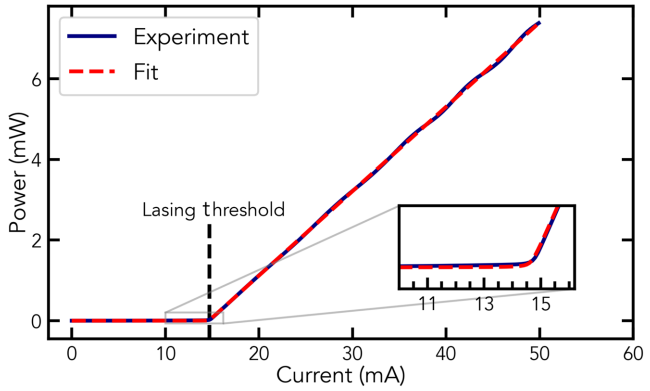

FIG. 5. Fit of the laser PI curve to Eq. (17), using F, I_s, and I_{th} as fit parameters. The inset shows a good fit around the lasing threshold $I_{\text{th}} = 14.7$ mA.

In total, the fitted parameters are $g, \tau_n, K, \alpha, f_c, F, I_s$, and I_{th}, giving eight constraints to the rate-equation parameters. There are ten rate-equation parameters, however V and Γ_a just reflect the choice of expressing the rate equations in terms of number or density of carriers and photons. They do not affect the simulation results, and so we can assume a reasonable value for each: $V = 2 \times 10^{-17}$ m^3 and $\Gamma_a = 0.2$. The remaining eight rate-equation parameters are fully constrained by the fitted parameters, and can be calculated using the relationships stated above: ε is calculated from f_c; then τ_p can be calculated from the K factor, ε and g; β is calculated from I_s and finally N_0 is calculated from I_{th}. Alternatively, the rate equations can be rewritten in terms of the fitted parameters [24]. The extracted rate-equation parameters for our laser, based on the measurements plotted in Figs. 3–5, are shown in Table I.

4. Comparison to experiment

To confirm the accuracy of the model and extracted parameters, we compare the model predictions to experimental measurements. For a given current $I(t)$ the rate equations can be solved numerically to simulate the power output of the laser. We use the ordinary rate equations, Eqs. (4)–(6), without noise terms since we are here interested in the average power output. We directly measure the current from the pulse generator and use this measurement to define $I(t)$ in the rate equations. We use a single-frequency sinusoidal current to minimize the effects of high-frequency parasitics from the laser circuitry and packaging. To model the finite-bandwidth (10 GHz) of the detector we apply a 10-GHz first-order, low-pass filter to the rate-equation solutions, which has the effect of reducing the amplitude of the relaxation oscillations.

TABLE I. The extracted rate-equation parameters, based on the measurements shown in Figs. 3, 4, and 5.

Parameters	Values	Description
τ_n (ns)	0.15	Carrier lifetime
τ_p (ps)	4.47	Photon lifetime
g ($\times 10^{-6}$ cm^{3}s^{-1})	1.70	Differential gain coefficient
ε ($\times 10^{-17}$ cm^3)	3.24	Gain compression factor
N_0 ($\times 10^{18}$ cm^{-3})	3.79	Carrier density at transparency
β ($\times 10^{-5}$)	4.44	Spontaneous emission factor
α	2.95	Linewidth enhancement factor
η	0.52	Differential quantum efficiency
V ($\times 10^{-11}$ cm^3)	2	Active layer volume
Γ	0.22	Mode confinement factor

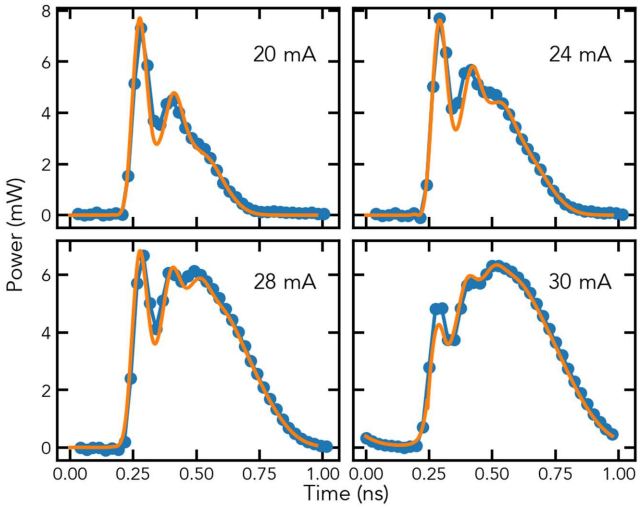

FIG. 6. Measured (dotted blue) and simulated (solid orange) laser pulses, at different bias currents (modulation current, 30 mA; repetition rate, 1 GHz).

Figure 6 shows a comparison between the simulated and measured intensity output of the laser when driven at a repetition rate of 1 GHz for different bias currents. There is a good agreement between experiment and simulation. The model correctly predicts the main features of the laser output: the steady-state power output, the turn-on delay and the amplitude, damping, and frequency of relaxation oscillations.

IV. MODELING LASER PHASE NOISE

Having verified the accuracy of the rate-equation model for simulating the power output of a gain-switched laser, we now turn to simulations of the laser phase noise. Recall that the phase noise is quantified by the variance $\langle \Delta\phi^2(t) \rangle$ of the Gaussian-distributed phase. We cannot derive an analytical expression for this quantity, and instead we employ the Monte Carlo method: we repeatedly solve the stochastic rate equations, and calculate the variance of the resulting distribution of phase values to estimate $\langle \Delta\phi^2(t) \rangle$. To verify the accuracy of this estimate we again compare the model predictions against experimental measurements.

We cannot measure phase directly, but we can indirectly measure $\langle\Delta\phi^2(t)\rangle$ by observing the distribution of intensities at the output of an asymmetric interferometer, like in Fig. 1 [35]. The experimentally observable intensity distribution depends on $\langle\Delta\phi^2(t)\rangle$, giving experimental access to this quantity. What is needed, therefore, is an analytical expression that relates the observable intensity distribution to $\langle\Delta\phi^2(t)\rangle$. Reference [35] achieves this by setting the fixed interferometer phase $\phi_0 = \pi/2$ and choosing a small interferometer delay such that $\sin(\Delta\phi) \approx \Delta\phi$. Equation (1) then becomes

$$I_{\text{out}} = \frac{I_{\text{in}}}{2}(1 + \Delta\phi) \tag{18}$$

such that the intensity is proportional to the phase and therefore the variance of the phase is simply proportional to the variance of the intensity, which can be measured. The shortcoming of this method is that it is limited to small phase-noise values for the small angle approximation to hold. We remove this constraint by using an analytical expression for the probability density function (PDF) of the intensity distribution for arbitrary phase-noise values. This PDF was derived in Ref. [36], and here we quote the result. Appendix A provides a full and intuitive derivation. Let $Y = \cos(\Delta\phi + \phi_0)$ be the normalized intensity, ignoring units and displacements along the x axis. Then the PDF of Y is

$$f_Y(y,\sigma) = \sum_{n=-\infty}^{\infty} \frac{1}{\sqrt{1-y^2}} \Big\{ f_{\Delta\phi}[2(n+1)\pi - \cos^{-1}(y) + \phi_0, \sigma^2] + f_{\Delta\phi}[2n\pi + \cos^{-1}(y) + \phi_0, \sigma^2] \Big\}, \tag{19}$$

where f_Y is the PDF of the normalized intensity, $f_{\Delta\phi}$ is the PDF of the Gaussian distribution (with zero mean) and $\sigma^2 = \langle\Delta\phi^2(t)\rangle$. As required, this expression relates the distribution of the phase $f_{\Delta\phi}$ to the experimentally accessible distribution of the intensity, f_Y. By fitting measurements of f_Y to Eq. (19) we can estimate $\langle\Delta\phi^2(t)\rangle$ by using it as a fitting parameter. Equation (19) includes an infinite sum, however, we can truncate the sum at $n = \pm 100$ with negligible effect on the results. One limitation of our method is that above a certain level of phase noise, f_Y becomes experimentally indistinguishable from an arcsine distribution. In fact, a wrapped Gaussian distribution with a large variance approaches a uniform distribution, so for large phase-noise values f_Y approaches an arcsine distribution. Therefore, our technique is limited to measuring phase-noise values below the threshold at which f_Y approaches an arcsine distribution. We find this happens around $\langle\Delta\phi^2(t)\rangle \approx 9$, which is in good agreement with previous results [7,20,36].

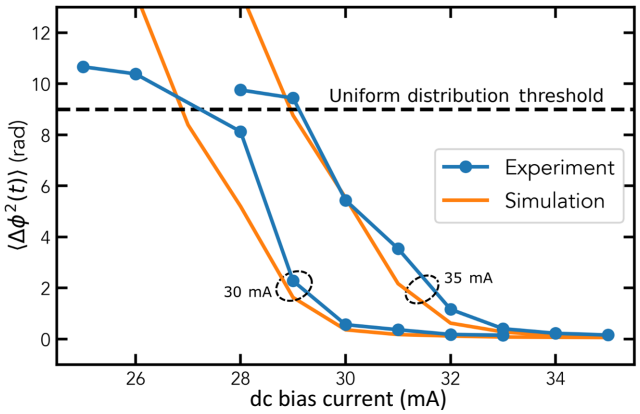

FIG. 7. Comparison between measured and simulated values of the phase noise $\langle\Delta\phi^2(t)\rangle$ as a function of bias current. Measurements are taken for two different modulation currents (30 and 35 mA), as indicated. The threshold at which the wrapped Gaussian phase distribution becomes approximately uniform is marked with a dashed line.

For our purposes this limitation is acceptable since we are exactly interested in determining whether the phase is approximately uniformly distributed, and hence do not need to measure higher phase-noise values.

Finally, we compare the model predictions with experimental measurements of the phase noise using the measurement technique just described. We perform a Monte Carlo simulation, calculating the laser phase evolution over one period (1 ns) 10 000 times by solving the stochastic rate equations under gain-switched conditions. We again use a measurement of the pulse generator output to define the current $I(t)$ in the stochastic rate equations. An estimate for $\langle\Delta\phi^2(t)\rangle$ is then given by the variance of the 10 000 solutions for $\Delta\phi$. We use this approach to estimate $\langle\Delta\phi^2(t)\rangle$ as a function of the laser dc bias current, at two different modulation currents (30 and 35 mA). Our simulation results are shown in Fig. 7.

To measure the phase noise, we gain switch the laser using the same current parameters as in the simulation, and measure the output power over 25 μs, corresponding to 25 000 pulses. We sample the intensity of each pulse and plot a histogram, which can be fit to Eq. (19), using $\langle\Delta\phi^2(t)\rangle$ as a fitting parameter. In our measurements we observe a slow drift of ϕ_0, on the order of rad/s, due to mechanical or thermal instabilities affecting the length difference between the short and long arm of the interferometer. This drift is much slower than our measurement time of 25 μs, so the effect on individual measurements is negligible. However, ϕ_0 can take on different values for measurements at different times, and to account for this we include ϕ_0 as another fitting parameter. Additionally we model classical sources of noise, such as electronic noise and laser intensity noise, with a Gaussian distribution

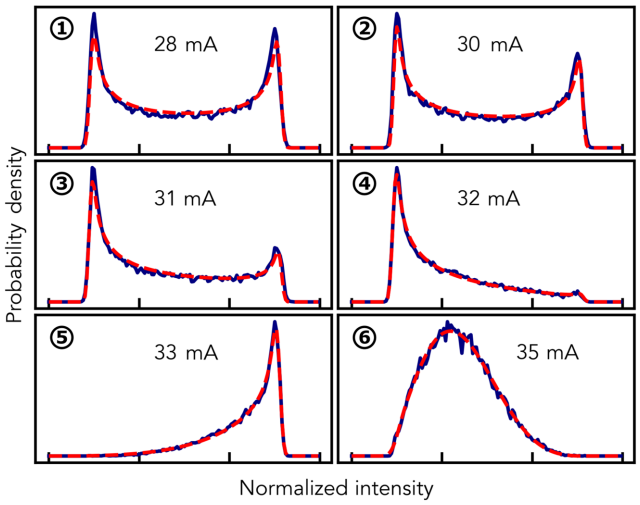

FIG. 8. Measured (solid blue) intensity distributions at different bias currents, fitted (dashed red) to Eq. (19). The effect of the slow drift of the relative interferometer phase ϕ_0 can be seen by most clearly comparing the intensity distributions at 32 and 33 mA. The peaks of the distributions are at different intensities, even when the phase noise is similar for both measurements.

independent from ϕ_0 or $\langle\Delta\phi^2(t)\rangle$. The total intensity distribution from classical and quantum sources is then given by the convolution of the Gaussian classical noise, and the intensity distribution due to phase noise f_Y. We include the variance of the Gaussian classical noise as a third fitting parameter.

Figure 8 shows examples of fitted intensity distributions for different bias currents of the laser, keeping other current parameters (modulation current, 30 mA; repetition rate, 1 GHz) constant. In Fig. 7 we plot the fitted values of $\langle\Delta\phi^2(t)\rangle$ alongside the simulation. We see that at low bias currents, the model predicts ever-higher phase-noise values, while our measurements plateau around $\langle\Delta\phi^2(t)\rangle = 9$. This corresponds to the level of phase noise at which the intensity distribution becomes indistinguishable from an arcsine distribution. At higher bias currents, with lower values of phase noise, we see a good agreement between experiment and simulation, verifying the accuracy of the model. Figure 7 clearly shows the point at which the Gaussian phase becomes approximately uniform: when the intensity distribution becomes indistinguishable from an arcsine distribution at lower bias currents, the measured phase-noise values plateau [around $\langle\Delta\phi^2(t)\rangle = 9$], while the simulation continues increasing. From our measurements we can therefore say that for a modulation current of 30 mA (35 mA), a bias current below approximately 26 mA (approximately 29 mA) is required to guarantee an approximately uniform phase, and hence the security of the QRNG.

V. EFFECTS ON PERFORMANCE

The effect of poorly selected laser driving parameters on the performance of a phase-noise-based QRNG can be made explicit by considering the min entropy associated to the interference signal. The min entropy quantifies the amount of identically and independently distributed (IID) bits in the digital codes, which are generated by an analog-to-digital converter (ADC) sampling the photodiode (PD) current signal. We consider an (ideal) ADC with a resolution of d bits and a measurement range of R volts, such that the range is divided into 2^d intervals of width $\Delta = R/2^d$. We associate the random variable W to the ADC output codes, each code corresponding to the index of the voltage interval into which the PD signal is measured at the time of sampling, i.e., $[w\Delta, (w+1)\Delta)$, with $w \in \{0, 1, \ldots, (2^d - 1)\}$. The min entropy of W is then defined as

$$H_{\min}(W) = -\log_2\left[\max_w P_W(w)\right], \tag{20}$$

where the discretized sample probability $P_W(w)$ is given by

$$P_W(w) = \int_{w\Delta}^{(w+1)\Delta} f_Y(y,\sigma)dy, \tag{21}$$

where f_Y is the PDF of the interference signal given by Eq. 19, allowing us to calculate the min entropy as a function of phase noise [36]. In the case of high phase randomization, the interferometer output intensity and therefore the amplitude of the PD signal, follows an arcsine distribution. In this case $\max_w P_W(w)$ corresponds to either the destructive or the constructive signal amplitudes, $Y = y_d$ and $Y = y_c$. For example, if y_d and y_c fall into intervals w and w', respectively, $\max_w P_W(w)$ will correspond to the largest between $\int_{y_d}^{(w+1)\Delta} f_Y(y,\sigma)dy$ and $\int_{w'\Delta}^{y_c} f_Y(y,\sigma)dy$. Ideally, in the absence of fluctuations and additive electronic noise, the distribution fits the whole range R such that codes $w = 0$ and $w = (2^d - 1)$ occur with the same discretized probability. Hence, if we assume a typical ADC resolution of $d = 8$, when the phase noise is uniformly distributed we obtain $H_{\min}(W) = 4.65$ bits.

We can now see how a nonuniform phase distribution will negatively affect the QRNG performance, by lowering the min entropy of the raw output distribution. Figure 9 plots the min entropy as a function of phase noise $\langle\Delta\phi^2(t)\rangle = \sigma^2$ with $d = 8$ and $\phi_0 = 0$. When the phase is not fully randomized, the resulting intensity distribution will become more asymmetric, as shown in Fig. 8. Crucially, this asymmetry will lead to a decreased min entropy: since one of the peaks in the distribution becomes larger, the probability of the most-likely outcome likewise increases. The physical reason for this behavior is that the smaller $\langle\Delta\phi^2(t)\rangle$ the less the phase changes from pulse

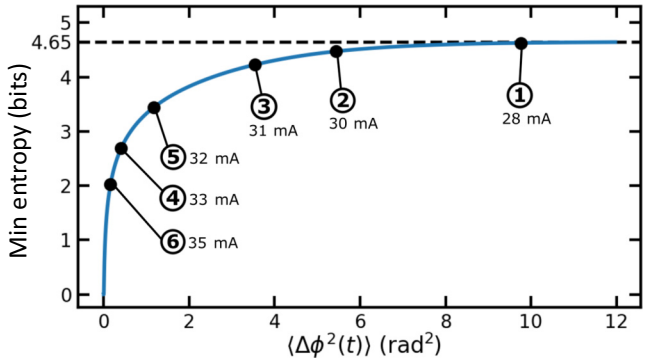

FIG. 9. Min entropy as a function of the phase noise, assuming 8-bit digitization resolution. The min entropy quantifies the extractable randomness of the QRNG and is proportional to the secure random-number generation rate. The numbers correspond to the measurements plotted in Fig. 8 at different bias currents, indicating a clear connection between the bias current, the phase noise, and the performance as quantified by the min entropy.

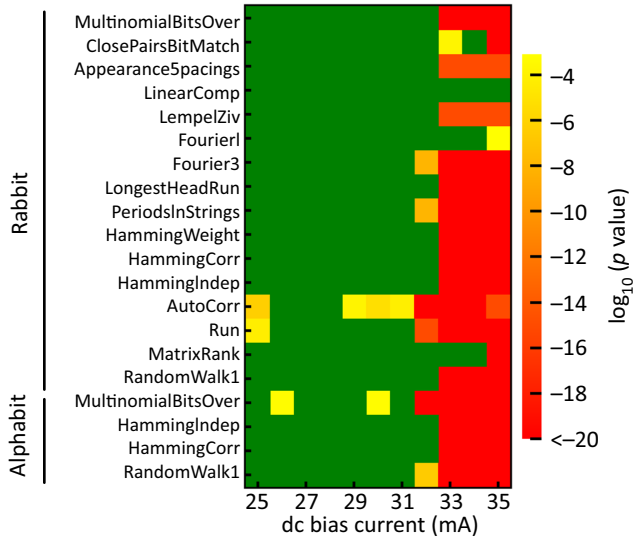

FIG. 10. The p values of different statistical tests from the TestU01 randomness testing suite applied to 1 GB of raw data from the QRNG at different bias currents. The bottom four tests correspond to the Alphabit battery of tests, and the rest are from the Rabbit battery of tests. Passed tests are drawn in green, and the p values of the failed tests (p value below 0.001) are indicated by the colorbar. Starting at 32 mA, the QRNG fails several tests with very low p values, indicating that the phase noise, and hence entropy, is too low for the unbiasing algorithm to completely remove bias and correlations from the generated numbers.

to pulse and hence the higher becomes the probability constructive and near constructive interference events.

We can combine this result with our simulations of the min entropy as a function of phase noise (Fig. 7) to directly relate the min entropy to the bias current. We indicate in Fig. 9 the points along the min-entropy curve corresponding to different levels of bias current, as measured in Figs. 7 and 8. In this way, combining the rate-equation simulations with the analytical calculations of the min entropy, we can quantify the effects on the performance of the QRNG as a function of the dc bias current directly, or any other current or laser rate-equation parameter.

Given the min entropy, the ADC output should be processed with a seeded randomness extractor, such as a two-universal hash function, in order to actually distill the IID bits from the samples [37]. It is worth stressing that $H_{\min}(Y)$ in Fig. 9 is not taking into account various factors such as dependencies among the samples, nonidealities of the ADC, electronic noise, laser fluctuations, so it overestimates the actual entropy content one would obtain in a realistic situation. However, since the postprocessed generation rate is proportional to the min entropy, Fig. 9 shows the critical loss of secure bits the QRNG user would experience in case the laser drifts away from the driving conditions that guarantee the larger phase randomization. In this situation, although the rate diminishes, the distilled random bits are secure as long as the randomness extractor is recalibrated on the actual min-entropy value.

This is not the case if instead of using a seeded randomness extractor, the user implements some unseeded postprocessing algorithm. We consider an unbiasing algorithm based on finite impulse response (FIR) filters [8,9,38], in which the unbiased output code $u(n)$ is given by scrambling together the last $n - M$ ADC codes $w(n)$, i.e., $u(n) = \sum_{i=0}^{M} b_i w(n-i) \mod 2^d$ where b_i are the coefficients of the filters. As FIR filter-based processing does not compress the raw random numbers, the generation rate is constant. This makes them a practical solution for applications such as Monte Carlo simulations, which consume a large amount of data but are less recommendable for cryptographic applications, since the generation rate does not depend on the actual min-entropy content.

As an experimental demonstration, we use the standard phase-noise QRNG setup from Fig. 1 with the laser operated at 1 GHz, the PD sampled at 1 GSsample/s by an ADC with 8-bit resolution, which we employ to generate 1 GB of raw output numbers at different levels of dc bias current while keeping constant the modulation amplitude. We then use the fifth-order FIR filter, i.e., $M = 4$ and with binomial coefficients $b_i = M!/i!(M-i)!$ [8] and analyze the results using the batteries *Rabbit* and *Alphabit* of the suite TestU01 for statistical randomness assessment [39]. These batteries are applied to the whole 8×10^9 bit long strings and Fig. 10 shows the test results at each level of bias current. As one can appreciate, when the laser is properly driven with low bias current, the FIR filter is very effective in unbiasing the output, since the tests output acceptable p values. However, starting at 32 mA, the QRNG begins to fail more tests and from 33 mA onward most of them fail catastrophically. Comparing these values

of bias current to Fig. 7 we see that at these levels of bias current, the phase noise is well below the uniform distribution threshold. So, again, the rate equations help determine the operational limits of dc bias current, or any other rate-equation parameter, required for the correct operation of the QRNG.

VI. DISCUSSION

The assumption of a uniform phase distribution due to spontaneous emission, leading to an arscine-distributed intensity, is fundamental to the security of phase-noise QRNGs. Our work puts this assumption on a stronger footing by quantifying the phase noise using a rate-equation model. Rate-equation modeling of laser diodes is a well-established technique from the field of classical optical communications, giving confidence that our analysis rests on solid foundations. We choose a parameter extraction technique based on a small number of simple measurements. Our method for measuring phase noise can be implemented with a standard phase-noise QRNG setup, with no need for additional equipment. This makes our analysis easy to replicate and implement as part of a certification process to guarantee the security of phase-noise QRNGs. Appendix B summarizes the steps outlined in this work to identify the operational limits of a phase-noise QRNG. Although we focus on quantifying the phase noise for the purposes of security, a rate-equation model has other useful applications. Here we describe two such potential applications.

We show how a rate-equation model can be used to quantify the phase noise in a gain-switched laser. Such a model can also be used to optimize the performance of a phase-noise QRNG, by selecting parameters to maximize the phase noise. The maximum sampling rate of the QRNG is limited by the time it takes for the laser to reach full randomization. Increasing the phase noise can therefore allow for higher sampling rates. Figure 7 shows that a 1 GHz gain-switched laser is able to achieve full phase randomization for appropriately selected current parameters. Our model can be used to investigate the maximum repetition rate at which the laser can be driven while still guaranteeing full phase randomization. The model also gives insight into which rate-equation parameters (intrinsic to the laser) affect the phase noise, notably α and β. Choosing a laser with a high value of α or β could again improve the maximum sampling rate. The effect of other rate-equation parameters is less obvious, but can similarly be investigated. Laser phase noise is not the only consideration for maximizing the QRNG performance. For example, laser chirp is a feature of directly modulated laser diodes, which can lead to low visibility interference at the interferometer output. It is especially problematic at high repetition rates and large intensity modulations. The rate equations can again be used to select current parameters such that the chirp is minimized, or to find a suitable trade-off between high sampling rate and high visibility interference.

Even if suitable parameters have been chosen for the operation of the QRNG, the device can malfunction or its performance can degrade over time. QRNGs, like RNGs in general, can also be the targets of hacking attacks. For these reasons it is helpful to monitor the behavior of the QRNG to detect malfunctioning or other deviations from normal behavior. The standard approach consists of running statistical tests on the generated numbers to detect correlations or other signs of nonrandomness. However, passing statistical tests of randomness is a necessary but not sufficient condition for establishing the correct operation of a QRNG. A seemingly random string of numbers can nonetheless be predictable and hence insecure (see, e.g., the "memory-stick attack" [40]). Having a strong understanding of the physical process by which the numbers are generated, backed up by a suitable model, is a more reliable approach to certifying the randomness of the output numbers. Our rate-equation model can serve to establish a baseline of correct operation to which the device behavior can be compared.

VII. CONCLUSION

In this work, we develop a laser rate-equation model for quantifying the phase noise of a gain-switched laser in a QRNG. We employ a parameter extraction method based on simple measurements, allowing us to quantitatively compare the model to experimental measurements. We find the model accurately predicts the power output and phase noise of the laser. By quantifying the phase noise using a model, we can give stronger guarantees that the generated numbers originate from quantum phase noise, improving the security of phase-noise QRNGs.

ACKNOWLEDGMENTS

V.L. acknowledges financial support from the EPSRC (EP/S513635/1) and Toshiba Europe Ltd. This work is supported by the Industrial Strategy Challenge Fund (ISCF): 106374-49229 Assurance of Quantum Random Number Generators.

APPENDIX A: DERIVATION OF EQ. (19)

We derive the PDF of the normalized intensity Y (f_Y) when the phase $\Delta\phi$ follows a Gaussian distribution ($f_{\Delta\phi}$). We first derive the cumulative distribution function (CDF) F_Y, and then differentiate it to obtain the PDF.

The CDF of $Y = \cos(\Delta\phi + \phi_0)$ is by definition

$$\begin{aligned} F_Y(y) &= \Pr(Y \le y), \qquad y \in [-1, 1] \\ &= \Pr[\cos(\Delta\phi + \phi_0) \le y]. \end{aligned}$$

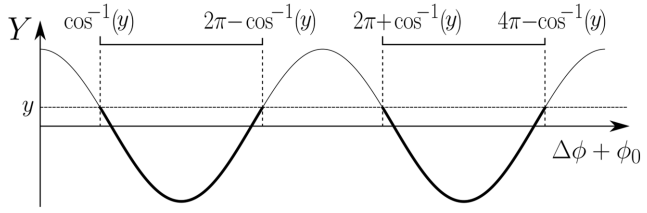

FIG. 11. Plot of the normalized intensity Y. The CDF of Y, $F_Y(y)$, is given by the probability that $\Delta\phi + \phi_0$ lies in one of intervals drawn in bold.

Figure 11 shows a plot of Y. The sections of the curve that are below y are drawn in bold. The probability that Y falls into one of these regions is therefore equal to the probability that the phase $\Delta\phi + \phi_0$ falls into one of the highlighted intervals on the x axis. These intervals occur every 2π radians and are given by

$$\begin{aligned}\Delta\phi + \phi_0 \in &[2n\pi + \cos^{-1}(y), 2(n+1)\pi - \cos^{-1}(y)]\\ \Delta\phi \in &[2n\pi + \cos^{-1}(y) - \phi_0,\\ &2(n+1)\pi - \cos^{-1}(y) - \phi_0],\end{aligned} \tag{A1}$$

where $n \in \mathbb{Z}$. The probability that $\Delta\phi$ lies in one of these intervals is given by

$$\begin{aligned}F_Y(y) = \sum_{n=-\infty}^{\infty} &\{F_{\Delta\phi}[2(n+1)\pi - \cos^{-1}(y) - \phi_0]\\ &- F_{\Delta\phi}[2n\pi + \cos^{-1}(y) - \phi_0]\},\end{aligned} \tag{A2}$$

where $F_{\Delta\phi}$ is the CDF of the Gaussian phase distribution. The last step is to differentiate both sides of the equation, using the fact that $d/dy(F_{\Delta\phi}) = f_{\Delta\phi}$ and $d/dy[\cos^{-1}(y)] = -1/\sqrt{1-y^2}$, to obtain Eq. (19):

$$\begin{aligned}f_Y(y,\sigma) = &\sum_{n=-\infty}^{\infty} \frac{1}{\sqrt{1-y^2}}\\ &\Big\{f_{\Delta\phi}[2(n+1)\pi - \cos^{-1}(y) - \phi_0, \sigma^2]\\ &+ f_{\Delta\phi}[2n\pi + \cos^{-1}(y) - \phi_0, \sigma^2]\Big\}.\end{aligned} \tag{A3}$$

APPENDIX B: EXPERIMENTAL PROCEDURE FOR FINDING THE OPERATIONAL LIMITS OF A PHASE-NOISE QRNG

We provide a step by step procedure for identifying the operational limits of a phase-noise QRNG, using a rate-equation model backed up by experiments.

1. *Implement the stochastic rate equations:* the equations can be solved using stochastic numerical integration, for example, with the Euler-Maruyama method.
2. *Extract the rate equation parameters:* (2a) measure the IM response of the laser at a range of bias currents (from approximately $1.2I_{\text{th}}$ to approximately $3I_{\text{th}}$). Subtract the lowest bias current measurement from the rest to obtain the subtracted IM response. Fit the subtracted response to Eq. (15) to measure f_r and Γ at each bias current. Plot Eqs. (12) and (13) using the fitted values to obtain estimates for g, the K factor, and τ_n. (2b) Measure the fiber transfer function at a bias current of approximately $2I_{\text{th}}$. Repeat the measurement removing the fiber from the system and subtract this measurement from the first. Extra attenuation should be added to the no-fiber setup to match the attenuation for both measurements. The NA should measure the same response at 0 Hz for both measurements. Fit the subtracted transfer function to Eq. (16) to obtain estimates for α and f_c. (2c) Measure the PI curve of the laser and fit to Eq. (17) to find estimates for F, I_s, and I_{th}. (2d) Use the fitted parameters to calculate the rate-equation parameters.
3. *Verify the extracted parameters:* measure the power output of the laser under gain-switched conditions, for different combinations of bias and modulation current. Use a sine wave modulation to reduce the effects of high-frequency parasitics from the laser circuitry. Separately, measure the output of the pulse generator and use this to define $I(t)$ in the rate equations. Solve the ordinary rate equations, without noise terms, with the extracted parameters to simulate the laser power output and compare this to the measurements.
4. *Use the model to establish operational limits:* for a range of bias and modulation currents, perform a Monte Carlo simulation of the phase noise. Solve the stochastic rate equations repeatedly, and record the change in phase over one period. Calculate the variance of the resulting phase values to obtain an estimate for $\langle\Delta\phi^2(t)\rangle$, which quantifies the phase noise. A value of $\langle\Delta\phi^2(t)\rangle > 9$ is required for the phase to be approximately uniformly distributed.
5. *Verify the operational limits:* using the phase-noise QRNG setup (Fig. 1), measure the intensity distribution at the output of the asymmetric interferometer. Fit this distribution to Eq. (19), with $\langle\Delta\phi^2(t)\rangle$ as a fitting parameter to measure the phase noise. Compare these measurements with the Monte Carlo simulation results.

[1] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, Quantum random number generation, npj Quantum Inf. **2**, 1 (2016).
[2] M. Herrero-Collantes and J. C. Garcia-Escartin, Quantum random number generators, Rev. Mod. Phys. **89**, 015004 (2017).

[3] Y. Liu, Q. Zhao, M. H. Li, J. Y. Guan, Y. Zhang, B. Bing, W. Zhang, W. Z. Liu, X. Yuan, H. Li, and *et al.*, Device-independent quantum random-number generation, Nature **562**, 548 (2018).

[4] Z. Cao, H. Zhou, X. Yuan, and X. Ma, Source-Independent Quantum Random Number Generation, Phys. Rev. X **6**, 011020 (2016).

[5] P. R. Smith, D. G. Marangon, M. Lucamarini, Z. Yuan, and A. Shields, Simple source device-independent continuous-variable quantum random number generator, Phys. Rev. A **99**, 062326 (2019).

[6] M. Jofre, M. Curty, F. Steinlechner, G. Anzolin, J. P. Torres, M. W. Mitchell, and V. Pruneri, True random numbers from amplified quantum vacuum, Opt. Express **19**, 20665 (2011).

[7] C. Abellán, W. Amaya, M. Jofre, M. Curty, A. Acín, J. Capmany, V. Pruneri, and M. W. Mitchell, Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode, Opt. Express **22**, 1645 (2014).

[8] Z. L. Yuan, M. Lucamarini, J. F. Dynes, B. Fröhlich, A. Plews, and A. J. Shields, Robust random number generation using steady-state emission of gain-switched laser diodes, Appl. Phys. Lett. **104**, 261112 (2014).

[9] D. G. Marangon, A. Plews, M. Lucamarini, J. F. Dynes, A. W. Sharpe, Z. Yuan, and A. Shields, Long-term test of a fast and compact quantum random number generator, IEEE J. Lightwave Technol. **36**, 3778 (2018).

[10] K. Petermann, *Laser Diode Modulation and Noise. Advances in Opto-Electronics* (Springer, Netherlands, 1988).

[11] G. P. Agrawal and N. K. Dutta, *Semiconductor Lasers* (Springer Science & Business Media, Boston, MA, 2013).

[12] G. Agrawal, *Lightwave Technology: Components and Devices* Vol. 1 (John Wiley & Sons, Hoboken, NJ, 2004).

[13] G. P. Agrawal, *Fiber-Optic Communication Systems* (John Wiley & Sons, Hoboken, NJ, 2012).

[14] L. Binh, *Optical Modulation: Advanced Techniques and Applications in Transmission Systems and Networks* (CRC Press, Boca Raton, Florida, 2017).

[15] C. Henry, Theory of the linewidth of semiconductor lasers, IEEE J. Quantum Electron. **18**, 259 (1982).

[16] C. Henry, Theory of the phase noise and power spectrum of a single mode injection laser, IEEE J. Quantum Electron. **19**, 1391 (1983).

[17] C. Henry, Phase noise in semiconductor lasers, J. Lightwave Technol. **4**, 298 (1986).

[18] 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**, 312 (2010).

[19] 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 (2012).

[20] T. Kobayashi, A. Tomita, and A. Okamoto, Evaluation of the phase randomness of a light source in quantum-key-distribution systems with an attenuated laser, Phys. Rev. A **90**, 032320 (2014).

[21] R. Shakhovoy, A. Tumachek, N. Andronova, Y. Mironov, and Y. Kurochkin, Phase randomness in a gain-switched semiconductor laser: stochastic differential equation analysis, (2020). ArXiv:2011.10401.

[22] I. Fatadin, D. Ives, and M. Wicks, Numerical simulation of intensity and phase noise from extracted parameters for CW DFB lasers, IEEE J. Quantum Electron. **42**, 934 (2006).

[23] G. Morthier and P. Vankwikelberge, *Handbook of Distributed Feedback Laser Diodes* (Artech House, London, 2013), 2nd ed.

[24] L. Bjerkan, A. Royset, L. Hafskjaer, and D. Myhre, Measurement of laser parameters for simulation of high-speed fiberoptic systems, J. Lightwave Technol. **14**, 839 (1996).

[25] K. Czotscher, S. Weisser, A. Leven, and J. Rosenzweig, Intensity modulation and chirp of 1.55-/spl mu/m multiple-quantum-well laser diodes: Modeling and experimental verification, IEEE J. Sel. Topics in Quantum Electron. **5**, 606 (1999).

[26] I. Tomkos, I. Roudas, R. Hesse, N. Antoniades, A. Boskovic, and R. Vodhanel, Extraction of laser rate equations parameters for representative simulations of metropolitan-area transmission systems and networks, Opt. Commun. **194**, 109 (2001).

[27] T. Erneux and P. Glorieux, *Laser Dynamics* (Cambridge University Press, Cambridge, UK, 2010).

[28] J. C. Cartledge and R. C. Srinivasan, Extraction of DFB laser rate equation parameters for system simulation purposes, J. Lightwave Technol. **15**, 852 (1997).

[29] R. Olshansky, P. Hill, V. Lanzisera, and W. Powazinik, Frequency response of 1.3 μm InGaAsP high speed semiconductor lasers, IEEE J. Quantum Electron. **23**, 1410 (1987).

[30] R. Hui and M. O'Sullivan, *Fiber Optic Measurement Techniques* (Academic Press, Cambridge, MA, 2009).

[31] G. E. Shtengel, R. F. Kazarinov, G. L. Belenky, M. S. Hybertsen, and D. A. Ackerman, Advances in measurements of physical parameters of semiconductor lasers, Int. J. Hi. Spe. Ele. Syst. **9**, 901 (1998).

[32] J. Wang and K. Petermann, Small signal analysis for dispersive optical fiber communication systems, J. Lightwave Technol. **10**, 96 (1992).

[33] R. Srinivasan and J. Cartledge, On using fiber transfer functions to characterize laser chirp and fiber dispersion, IEEE Photonics Technol. Lett. **7**, 1327 (1995).

[34] K. Hinton and T. Stephens, Modeling high-speed optical transmission systems, IEEE J. Sel. Areas in Commun. **11**, 380 (1993).

[35] B. Daino, P. Spano, M. Tamburrini, and S. Piazzolla, Phase noise and spectral line shape in semiconductor lasers, IEEE J. Quantum Electron. **19**, 266 (1983).

[36] M. W. Mitchell, C. Abellan, and W. Amaya, Strong experimental guarantees in ultrafast quantum random number generation, Phys. Rev. A **91**, 012314 (2015).

[37] D. R. Stinson, Universal hash families and the leftover hash lemma and applications to cryptography and computing, J. Combin. Math. Combin. Comput. **42**, 3 (2002).

[38] I. Kanter, Y. Aviad, I. Reidler, E. Cohen, and M. Rosenbluh, An optical ultrafast random bit generator, Nat. Photonics **4**, 58 (2010).

[39] P. L'Ecuyer and R. Simard, TestU01: A C library for empirical testing of random number generators, ACM Trans. Math. Softw. **33**, 1 (2007).

[40] A. Acín and L. Masanes, Certified randomness in quantum physics, Nature **540**, 213 (2016).