optics

MDPI

Article

Operation of an Electrical-Only-Contact Photonic Integrated Chip for Quantum Random Number Generation Using Laser Gain-Switching

Seán Ó Dúill [1,*], Leidy Rodriguez [1], David Alvarez-Outerelo [2], Francisco J. Diaz-Otero [2], Ankit Sharma [3], Frank Smyth [3] and Liam P. Barry [1]

[1] Radio and Optics Research Laboratory, School of Electronic Engineering, Dublin City University, Glasnevin, D09 V209 Dublin, Ireland
[2] AttlanTTic Research Center, University of Vigo, EI Telecommunication, 36310 Vigo, Spain
[3] Pilot Photonics Ltd., Invent Building, Dublin City University, Glasnevin, D09 V209 Dublin, Ireland
* Correspondence: sean.oduill@dcu.ie

Abstract: We present the results of the detected voltage distribution of a quantum random number generator (QRNG) based on a photonic integrated circuit comprising a semiconductor laser, delay interferometer and photodetector. We find that the integrated QRNG system behaves as expected for a QRNG from discrete gain-switched laser sources, especially exhibiting all of the peculiarities of the random voltage distribution and behaving as previously demonstrated for a discrete optical component setup. The biggest advantage of having all of the components integrated into a single chip is that only electrical connections are needed to operate the system, without the need for tricky and expensive optical alignment to external circuitry. We supply results showing that a random bit stream created from the random numbers passes the NIST statistical test suite tests, thus demonstrating the feasibility to generate random numbers via quantum means at gigabit/s rates from a single photonic integrated circuit. All of our results are backed by numerical simulations.

Keywords: random number generation; integrated photonics; photonics integrated circuit; laser; noise; modulation; quantum effects

Citation: Ó Dúill, S.; Rodriguez, L.; Alvarez-Outerelo, D.; Diaz-Otero, F.J.; Sharma, A.; Smyth, F.; Barry, L.P. Operation of an Electrical-Only-Contact Photonic Integrated Chip for Quantum Random Number Generation Using Laser Gain-Switching. *Optics* **2023**, *4*, 551–562. https://doi.org/10.3390/opt4040040

Academic Editor: Francesco Chiavaioli

Received: 19 September 2023
Revised: 18 October 2023
Accepted: 23 October 2023
Published: 27 October 2023

1. Introduction

Random number generation is becoming increasingly important in the modern world for security, cryptography, communication and simulation applications. A class of random number generators based on a purely quantum physics phenomenon is highly desired due to the underlying indiscriminate randomness enabling a significant level of entropy [1–3]. Random numbers can be generated electronically, exploiting physical metastability within electronic circuits [4–6] and/or exploiting numerical algorithms on digital processors [7].

Photonic techniques can also be used to create random numbers, e.g., random phase diffusion in imaging [8], chaos in external-feedback lasers [9], chaotic regimes of wideband optical frequency combs [10,11], random effects within fiber lasers [12] and vacuum fluctuations in semiconductor lasers [13]. In recent years, generating quantum random numbers using laser gain-switching [14] has attracted considerable interest [15–18], especially arising from the quantum-event nature of spontaneous emission to seed new pulses every modulation cycle as the underlying process to create a QRNG.

Laser gain-switching is the periodic switching of a laser above and below a threshold to create a periodic optical pulse train, with pulses of picosecond duration shorter than the electrical pulse that drives the laser [19–22]. Gain-switching of semiconductor lasers has been extensively studied over the previous decades for picosecond pulse generation [19–22], optical time division multiplexing [21] and recently, as an optical frequency comb source for telecommunications and sensing applications [22]. The condition allowing for random

number generation via gain-switching is when each pulse in the pulse train has no memory of the optical phase of previous pulses in the pulse train [14,15]. In our previous studies of laser gain-switching for optical frequency comb generation, we showed that when each pulse has no phase memory with a uniform pulse-to-pulse phase distribution from 0 to 2π, the pulse train exhibits no comb lines in the optical spectrum [23], and such conditions occur when the laser is being sinusoidally modulated at a frequency much smaller than the natural relaxation frequency of the laser, whereby each pulse is created by spontaneous emission (SE) in the laser cavity at the instance when the round trip gain increases from below to above the threshold. The previous statement is true irrespective of the intrinsic linewidth value the laser possesses in CW operation. The random optical phase needs to be converted into an electrical signal for practical operation, so the pulses are sent into a delay interferometer (DI), with the delay equaling the gain-switching repetition period; the delay interferometer also possesses voltage-controlled coupling so that the pulse amplitudes from both arms of the interferometer are equal in magnitude when re-combined. The coherent addition of adjacent pulses transforms the random phase into random voltage fluctuations in a photodiode, thus, the coupling control of the interferometer maximizes the dynamic range of the QRNG signal. Interferometers operating with delays of hundreds of picoseconds require a length of waveguide, with a group refractive index of ~3.5, approaching 100 mm. Adding connectors and maintaining polarization stability can be problematic with a discrete component setup; therefore, an integrated solution combining lasers, delay interferometers and photodiodes is desired. Integrating lasers, adjustable delay interferometers and photodiodes onto the same photonic integrated circuit (PIC) is the only way to achieve stable operation with the attraction of creating a compact QRNG source for wider system deployment [24].

In this paper, we show the full functionality of a PIC designed for QRNG using laser gain-switching [24]. A schematic of the PIC and constituent components is shown in Figure 1. The PIC is mounted on an RF subcarrier to allow for high-speed radio frequency (RF) connections, DC current laser bias connections, and DC voltage tuning of the DI to equalize the optical power in each arm at the recombination arms of the DI and potentially provide for long-term stability of the QRNG system; these are the only physical connections made with the PIC. All of the lightwave processing is performed on-chip, which makes for a robust and simplified QRNG source. The system is optimized for QRNG by creating the largest distribution of random voltages at the photodetector. We find that gain-switching the laser at 1.25 GHz corresponds to the operating frequency of the delay interferometer. We present eye diagrams of the pulsating output from the PIC for various laser bias currents, as well as the corresponding distribution of the detected voltages. We find that the behavior of the voltage distribution is as expected for QRNG via gain-switching, including the hallmark change in voltage distribution pattern as the bias current is increased to the point where the laser pulses are no longer seeded by SE and hence lose QRNG ability [15]. We take one of the measured output pulsation waveforms to generate a random bit stream that, as we show, passes the NIST statistical test suite (STS) [25].

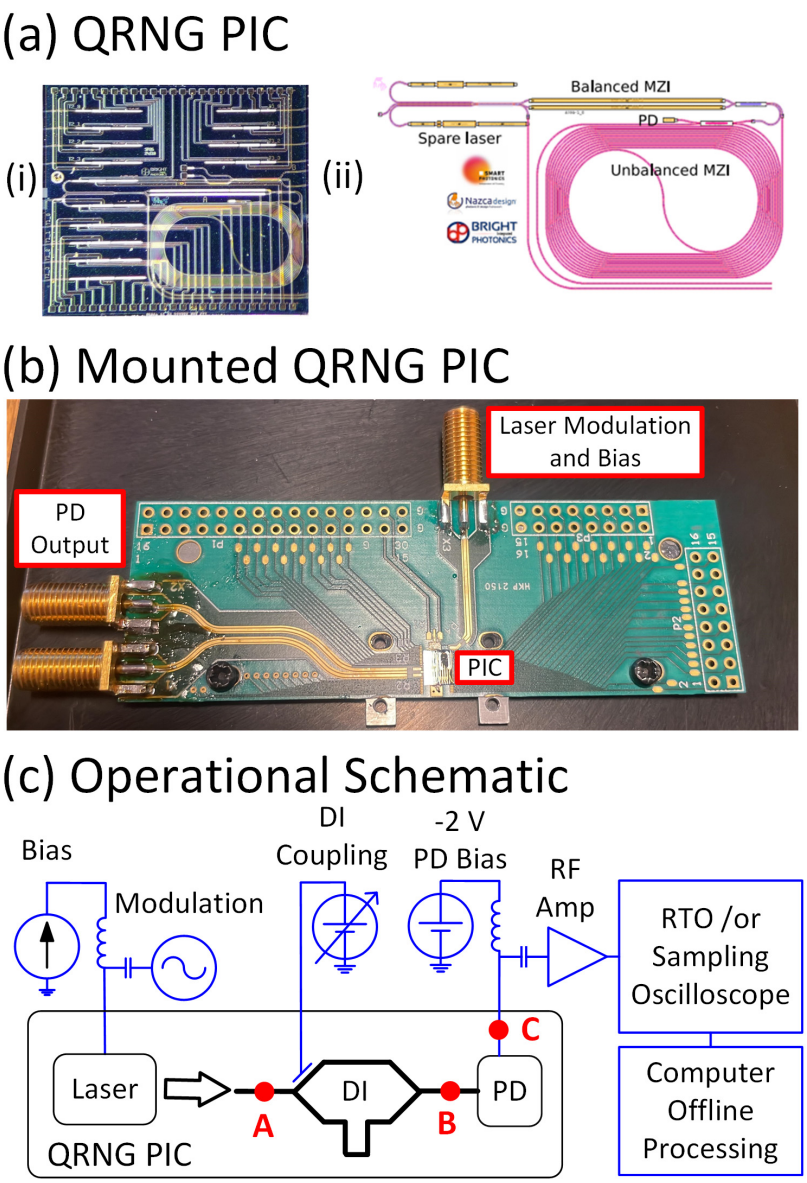

Figure 1. (**a**) (**i**) Photograph of the QRNG PIC; (**ii**) constituent components of the QRNG PIC. (**b**) Photograph of the mounted PIC on the RF test board showing the input port for laser biasing and modulation, and the output port from where the PD signal emerges. Apart from a separate DC voltage to control the delay arm in the MZ splitter, no other physical connections are needed. (**c**) Operational schematic of the QRNG PIC and the experimental setup. Light pulses are created by modulating the laser; the pulses are then split, with the pulse in the upper arm experiencing a one modulation period delay and recombined with the pulse travelling in the lower arm, thereby transforming the random phase into random amplitude fluctuations. The PD signal is sent off-chip and electrically amplified before processing to create a random bit stream.

2. Device and Experimental Setup

Full details of the PIC have previously been published [24]; here, we summarize the important features. A schematic of the PIC, the mounted PIC on a RF test board, and the experimental setup is shown in Figure 1a–c, respectively. Only the basic functional schematic of the DI is shown in Figure 1c. The actual DI (denoted as an unbalanced MZI in Figure 1a) implemented on the PIC is slightly more complicated to allow for compensating optical losses of 19.6 dB [24] in the delay arm, while maintaining optical power balancing from each arm at the photodiode. The DI requires a differential distance of 64.4 mm [24]

between each arm to produce an 800 ps differential delay; the losses accrued by the pulses traversing the delay arm are considerable and are about 19.6 dB [24]. To balance the power at the PD, the pulses from the laser first go through a balanced MZI (Figure 1a) with a differential DC voltage control phase shifter that alters the optical power split ratio into each arm of the DI (unbalanced MZI). The PIC is built upon an InP substrate with a distributed feedback laser, Mach–Zehnder interferometer and photodetector integrated onto the same photonic chip. The PIC is mounted on a RF test board, shown in Figure 1b, with ~10 GHz RF bandwidth that suffices for the purposes of this study. The laser gain-switching RF signal is a +13 dBm RF sinewave at a frequency of 1.25 GHz and is electrically coupled using a bias tee with the DC laser bias current, from just above threshold to three times threshold, and applied to the coaxial connector for laser modulation and bias on the board. The electrical signals travel via RF strip line circuitry that is wirebonded to the laser. The photodiode output is wirebonded to another strip line RF waveguide and then connected to an external bias tee configured to apply a -2 V voltage to the photodiode, as well as amplifying the random amplitude pulsation signal. The pulsations are observed on a sampling oscilloscope which facilitates the optimization of the random signal. The random signal is optimized for the largest voltage swing by varying the modulating frequency, drive amplitude and DI bias. In order to investigate the distribution and test for randomness, the pulsation output is recorded using digital real time oscillography, with four million voltage samples taken at 10 GSa/s.

In an initial numerical study, to obtain a better understanding of the process, we used the same stochastic laser model as described in our previous works; the equations and parameters are given in Appendix A. The simulated optical signal at specifically identified points along the PIC from Figure 1c are presented in Figure 2, showing laser pulsation, random amplitude pulsation after the DI and the lowpass filtered pulsation signal.

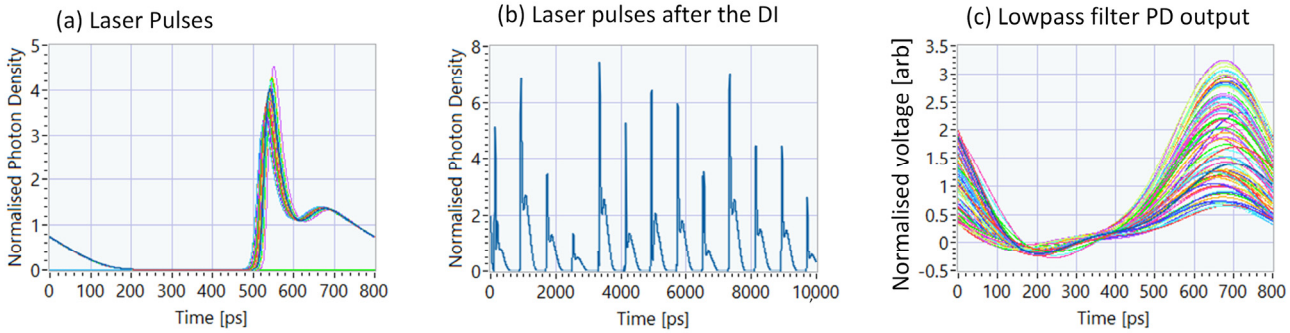

Figure 2. Simulated eye-diagrams at the various points indicated by a red dot · in Figure 1c. (**a**) Point A Laser pulse: regular pulsations from gain-switching the laser. (**b**) Point B Laser pulses after the DI: intensity of thirteen consecutive pulses after the DI to highlight the random amplitude of the pulses. (**c**) Point C Lowpass filter PD output: eye diagram of the pulse train containing the QRNG signal, each different color curve indicates a separate modulation period. Note that the pulses have undergone an electrical lowpass filtering with 2.5 GHz bandwidth to generate part (**c**).

To show the QRNG properties, a random bitstream is created from the voltage waveform at a high laser bias, with maximum range of random voltage, and passed through the NIST STS tests.

3. Results

We now present the results of the amplified PD voltage to show the voltage distribution of the QRNG signal from the PIC. We show the measured eye diagram from the sampling oscilloscope first because this shows exactly where the QRNG signal exists in the received signal. We then show the PD voltage distribution of the detected QRNG signal along with PD voltage distributions from a numerical laser simulator. Finally, we report on the results of the generated QRNG bit pattern through the NIST STS program [25].

3.1. Sampling Oscilloscope Eye Diagrams

A sampling oscilloscope of 30 GHz electrical bandwidth is synchronized by tapping off 10% of the RF power from the RF driving signal to trigger the sampling oscilloscope. The amplified PD output is then captured by the sampling oscilloscope (note that the voltage is inverted after the amplifier). In the eye diagram mask mode, the oscilloscope overlays detected voltage waveforms over two modulation periods. Each eye diagram plot is the accumulation of voltage values detected over a duration of at least two minutes. The eye diagrams for nine different laser bias currents are shown in Figure 3. For each scenario, there exists one signal sampling instance per modulation cycle that yields a large random voltage distribution, as indicated in Figure 3d. As is clear from the trend in all of the diagrams in Figure 3, the voltage distribution range increases with increasing laser bias current, which is expected for QRNG signals from delayed interference gain-switched laser topology [15]. There is, however, a maximum bias for which a random amplitude pulsation exists, because at larger biases, the RF drive signal may not be strong enough to drive the laser below threshold and hence fails to quench each pulse before the generation of the following pulse; we see this in our results for 34 mA and beyond.

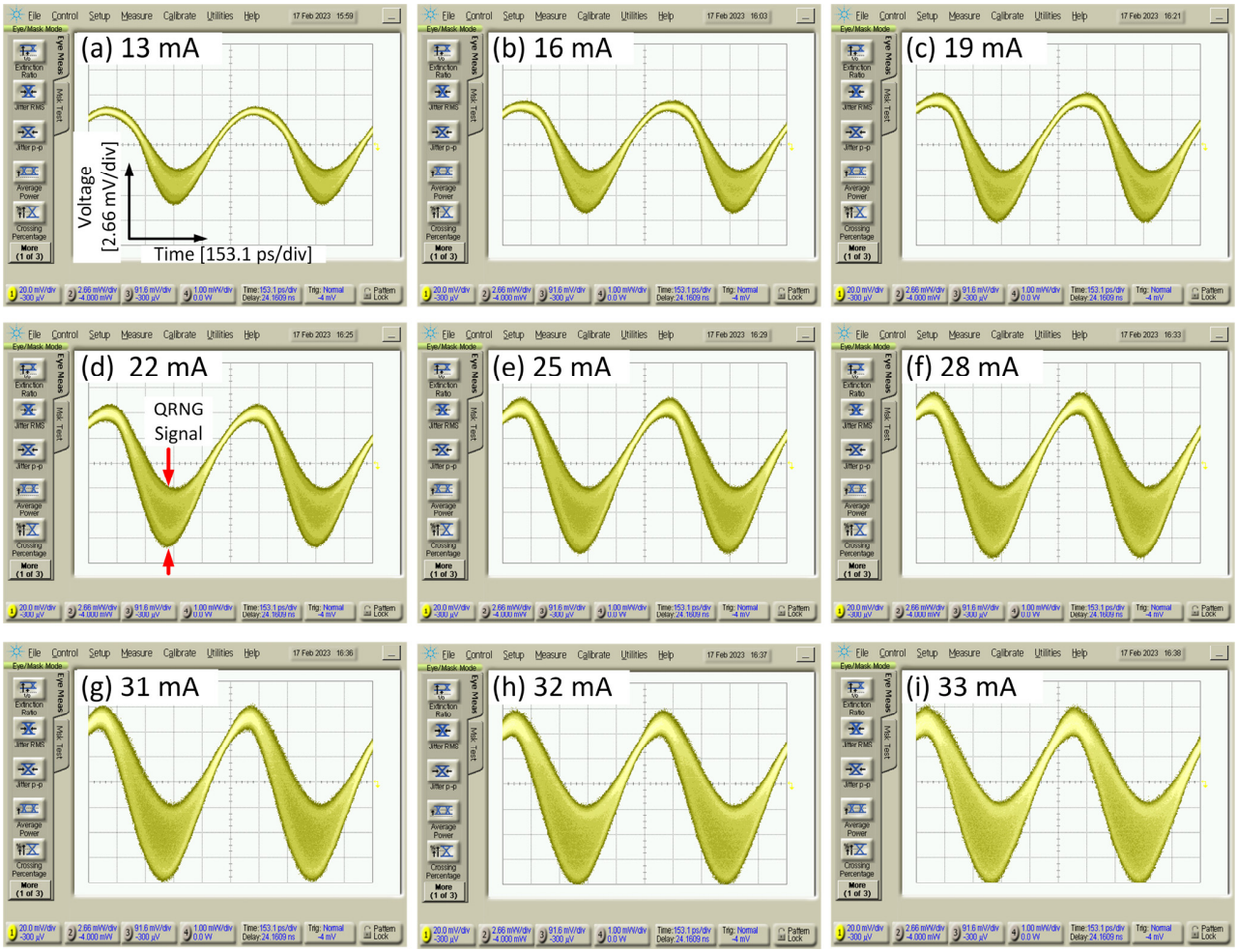

Figure 3. (**a**–**i**) Screenshots of eye diagrams of the PD output taken by a sampling oscilloscope for each of the laser bias currents indicated in each subplot; the eye diagrams correspond to the voltage distributions in Figure 2c. Each eye-diagram shows many thousands of overlaid sampling points taken over a two minute duration. The QRNG signal is explicitly indicated by the red arrows for subplot (**d**) though the concept applies equally for all subplots (**a**–**i**), the red arrows indicate the random variation of voltages at the relevant sampling instance.

3.2. QRNG Voltage Distribution

To measure the voltage distribution, we swapped the sampling oscilloscope for real time oscillography (RTO) because the sampling technique of the sampling oscilloscope only takes samples at different relative timings of the signal over many periodic cycles of the signal, hence, the sampling oscilloscope traces can only indicate the possible range of values of the QRNG signal. The RTO bandwidth and sampling rate are 2.5 GHz and 10 GSa/s, respectively. Since the frequency of the modulating signal is 1.25 GHz and the sampling rate is 10 GHz, we therefore captured eight samples per modulation period. A total of four million samples were captured which was the limit of the RTO employed, yielding a total of 500,000 QRNG voltage samples per detected RTO waveform.

In our scenario, the QRNG signal is the minimum detected voltage within a block of 16 samples from the upsampled RTO waveform, and the QRNG signal is built up by selecting the minimum voltage over every modulation period, which is 16 samples in our case. The voltage distributions with increasing laser bias current are shown in Figure 4. Note the presence of all of the hallmarks of the QRNG obtained by laser gain-switching and compared with the general trend established in [15]: (i) the increase in the range of voltage as the bias current is increased, (ii) the sharp cutoff in voltage outside the range of detected voltages, (iii) characteristic peaks at both ends of the voltage range arising from phase to amplitude conversion from the DI and (iv) the change in the distribution from being centered around the lower voltage peak to being centered around the higher voltage peak as the bias current increases from 32 mA to 33 mA in Figure 4h,i. Note that at sufficiently high bias currents (34 mA and higher), the RF signal can no longer gain-switch the laser below the laser threshold, and there is no wide range voltage distribution.

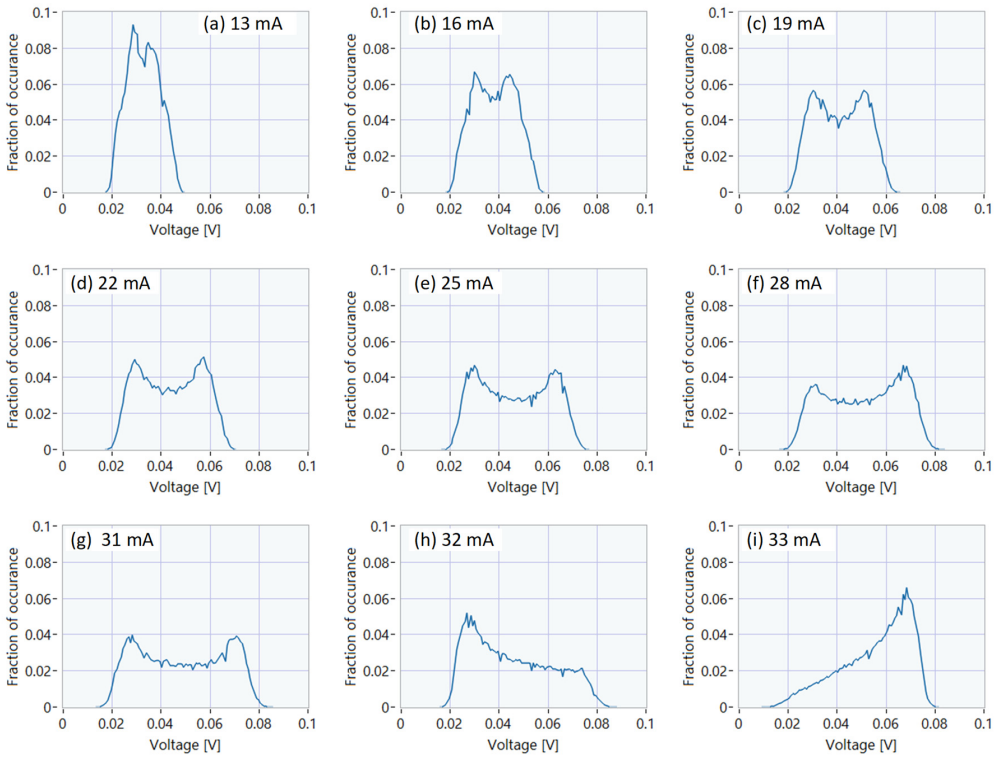

Figure 4. (**a**–**i**) Distributions of the measured voltage maxima during each modulation period for the value of laser bias current indicated in each subplot. As expected, each distribution is almost flat, except for the peaks at the extremities for the cases (**a**–**g**). The range of random voltages increases with increasing bias from (**a**) 13 mA up to 31 mA in (**g**); for larger bias currents, the modulating signal is insufficiently strong to gain-switch the laser. For the cases of 32 mA (**h**) and 33 mA (**i**), the bias is increased so that the laser is not being gain-switched and the voltage distribution is skewed to the low voltage level in (**h**), and then, it is skewed to a higher voltage level in (**i**).

3.3. Results of the NIST STS Tests

We concentrate on analyzing the QRNG signal for the case of laser bias at 22 mA (Figure 4d) because this is mid-range between the laser threshold current (~11 mA) and the maximum laser bias allowing for QRNG signal generation (33 mA). To remove quantization effects from the low voltage amplitude signal of the RTO, the RTO waveform is upsampled by a factor of two and interpolated, now giving 16 samples per modulation period. We take the upsampled RTO trace and convert it to random bits by applying a binary decision threshold at 0.0464 V and creating a copy of the QRNG bit stream, applying a circular shift of 100,000 samples to the copy and then applying an exclusive OR operation with the original QRNG bit stream. The NIST STS tests are applied to the output bit stream. We found that the QRNG bit stream passed all of the tests, with the *p*-values arising from each test shown in Figure 5. The comprehensive results of the STS tests are given in the Supplementary Materials, and we disclose the following for independent verification: complete results files of the NIST STS tests; the upsampled RTO trace; the bit stream generated after binary thresholding; and the delayed and XOR bit stream that is then used as input to the STS tests. Even though we have generated one random bit per voltage sample, the minimum entropy from this system is $-\log_2(p_{max})$, where p_{max} is the highest probability of occurrence for any random voltage. From Figure 4d, p_{max} is ~0.05; therefore, the minimum entropy from the source is 4.32 bits.

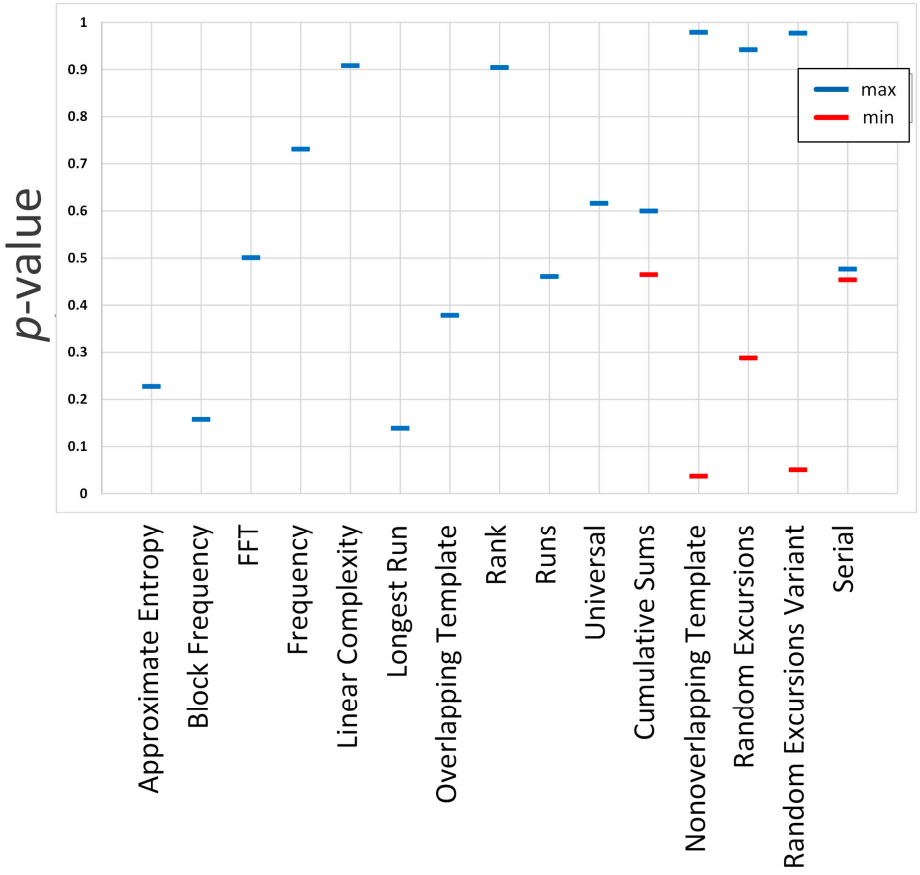

Figure 5. The calculated *p*-values of each of the NIST STS tests. For entries with two values, the maximum and minimum *p*-values of the relevant tests are shown. The folder containing the complete results of the STS tests are given in the Supplementary Materials. Note that all of the tests scored a *p*-value > 0.05 and hence passed the tests.

3.4. Simulation Results of the QRNG Signal

For completeness, we present simulated PD voltage distributions arising from the laser gain-switching with a delay interferometer. We take the complex-valued laser field [26]

model that we have used extensively to simulate laser gain-switched systems [23,27]. The details are in Appendix A. The laser field equations are much preferred for use in this scenario, rather than having separate rate equations for photon density and laser phase, because of the difficulty in correctly adding random photons when the laser photon density goes to zero, i.e., employing random numbers from a Gaussian distribution can drive the photon density toward negative, yielding non-physical results. We acknowledge the lack of a small correlation between the random carrier density and laser photon density when considering the complex-field approach; the results we present show that the complex-valued field rate equation suffices to capture the main peculiarities of the gain-switched QRNG system.

The total system simulator comprises a laser simulator considering lumped rate equations which consider stochastic sources for the carrier density and spontaneous emission. A delay interferometer that shifts and adds a quadrature rotated (multiply the complex field by '*j*') laser field, *E*, shifted by precisely one modulation period; the laser modulation frequency should be adjusted to produce an integer number of laser samples over one modulation period, i.e., the numerical sampling frequency should be an integer multiple of the RF modulation signal. The PD voltage is proportional to $|E|^2$ followed by a tenth-order Butterworth lowpass filter, with bandwidth twice that of the modulating signal. The optimum sampling instance is obtained by taking 100 arrays, with each array having a duration of one full modulation period. The index at which the maximum voltage is found for each array, the most frequent index obtained from the 100 arrays, becomes the offset at which the RNG sample is taken from each modulation period. We simulated over 100,000 modulation periods, thus collecting 100,000 RNG samples from the simulator. Histograms of the simulated RNG voltages are obtained and plotted in Figure 6.

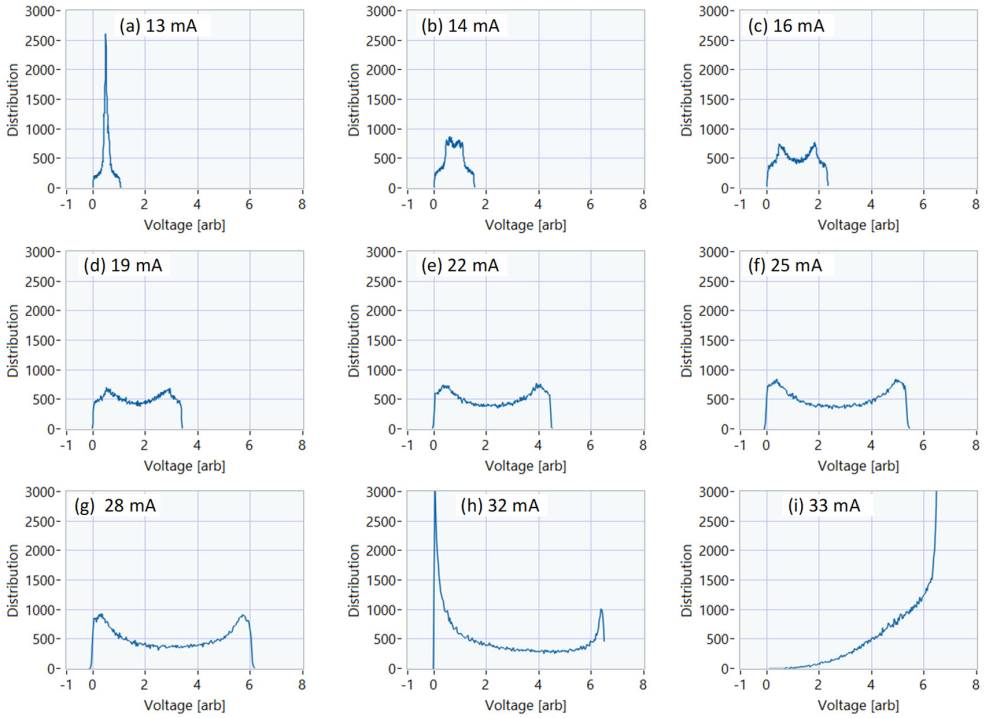

Figure 6. (**a**–**i**) Simulated RNG voltage distributions from the gain-switched laser and delay interferometer system for each value of laser bias current as indicated in each subplot. Note that the voltage distributions follow the same trend as for the experimental voltage distributions from the PIC in Figure 4.

The simulations were performed at various laser bias current levels as per the experiments. We find that the simulation yields similar voltage distributions as per the experiments, including the peculiarities of (i) increased voltage distribution with respect to

bias, (ii) peaks at each side of the distribution, (iii) sharp fall-off in the voltage at the lowest and largest voltages and (iv) the swing to lower and higher edges of the distribution as the bias current is increased, such that the laser is no longer being gain-switched. There is good qualitative agreement between the simulations and the experiments across the range of bias currents, apart from the case at low bias currents of 13 mA where just a single peak is visible in the voltage distribution of Figure 6a. The single peak splits off into two peaks as the bias current is increased.

4. Discussion

We have shown conclusively that a PIC containing a gain-switched laser and delay interferometer with only electrical and RF bond wire connections can produce a QRNG signal. We have verified that voltage distributions are as expected with similar QRNG systems with discrete lasers and delay interferometers. The results are confirmed by performing a numerical simulation of the entire laser and delay interferometer system.

One aspect of the experiment that we did not highlight is that the PIC itself was operated without any thermoelectric control. This in itself prompts an investigation into the long term stability of this system to produce a QRNG signal; without expensive thermoelectric control, this should be feasible because of the low RF drive power needed to create the laser pulsations and hence should be able to produce a robust QRNG system in a small form factor package.

5. Patents

Francisco J. Díaz Otero, David Álvarez Outerelo, "Generador cuántico de números aleatorios", Spain, no. PCT/ES2021/070179, 7 October 2021.

Supplementary Materials: The following supporting information can be downloaded at: https://www.mdpi.com/article/10.3390/opt4040040/s1. Filename datasets.zip. The RTO waveform, the bitstream generated after thresholding, the bit stream after the delay and XOR function applied. The entire contents of the NIST STS results folder are supplied.

Author Contributions: Conceptualization, L.P.B., D.A.-O. and F.J.D.-O.; methodology, S.Ó.D., L.P.B., D.A.-O. and F.J.D.-O.; software, S.Ó.D.; validation, S.Ó.D., L.R., D.A.-O., F.J.D.-O. and L.P.B.; formal analysis, S.Ó.D. and L.R.; investigation, S.Ó.D., A.S. and L.P.B.; resources, L.P.B., D.A.-O., F.J.D.-O. and F.S.; data curation, S.Ó.D.; writing—original draft preparation, S.Ó.D. and L.P.B.; writing—review and editing, S.Ó.D., L.R., D.A.-O., F.J.D.-O., A.S., F.S. and L.P.B.; visualization, S.Ó.D., A.S. and D.A.-O.; supervision, L.P.B., D.A.-O. and F.J.D.-O.; project administration, L.P.B.; funding acquisition, L.P.B., D.A.-O. and F.J.D.-O. All authors have read and agreed to the published version of the manuscript.

Funding: Funding for this work was provided for by the Science Foundation Ireland through project 12/RC/2276_P. and EU Horizon 2020 through the following projects: MSCA Agreement No. 847652, and MSCA H2020-ITN-2018-EDIFY (Contract number 813467).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: We make available the RTO waveform, NIST STS test results folder and QRNG bit sequences for independent verification.

Acknowledgments: The Galician Regional Government (consolidation of Research Units: AtlantTIC).

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

We provide details of the simulated QRNG system. The main model is that of the stochastic model for semiconductor lasers [25]. We have used this model in many previous works to study optical frequency comb generation and for laser injection locking phenomena [23,27]. The complex-valued envelope of the laser optical field is used to avoid numerical instability issues when the squared magnitude of the laser field (photon density)

results in zero under gain-switching, such that the stochastic spontaneous emission terms do not erroneously make the photon density have a negative value.

$$\frac{dN}{dt} = \frac{I_{bias} + \Delta I \sin(2\pi f_{mod} t)}{eV} - R(N) - \frac{a(N - N_0)}{1 + \epsilon_{nl}|E|^2}|E|^2 + F_N \tag{A1}$$

$$\frac{dE}{dt} = \frac{(1 - j\alpha_H)}{2}\left[\frac{a(N - N_0)}{1 + \epsilon_{nl}|E|^2} - \frac{1}{\tau_P}\right]E + F_E \tag{A2}$$

where all of the symbols have their usual meaning and are defined in Table A1. The carrier density is given by N, and E is the envelope of the laser optical field and related to the photon density in the laser. The first term on the right hand side of (A1) represents the laser bias and sinusoidal modulating current. Carrier recombination is given by $R(N) = AN + BN^2 + CN^3$ for non-radiative, bimolecular and Auger recombination, respectively; the third term represents stimulated emission. E is a complex-valued quantity describing the envelope of the optical field and encompasses all amplitude and phase modulation effects imposed by gain-switching; E is normalized such that $|E|^2$ represents the photon density of the laser field. F_N denotes stochastic carrier recombination (which will be defined later). The first term on the right-hand side of (A1) describes the complex gain of the laser field. The gain coefficient is given by $a(N - N_0)$, where a is the differential gain and N_0 is the carrier density at transparency. τ_P is the cavity lifetime. The final term F_E is the random addition of spontaneous emission due to bimolecular recombination into the lasing field, denoting spontaneous emission into the lasing field.

The stochastic terms are appropriately scaled for numerical computation (A1) and (A2) with $B_{sim} = t_s^{-1}$, where t_s is the step time. We solve the system of equations using Huen's predictor-corrector method.

$$F_N = \sqrt{2R(N)B_{sim}}e_N(t) \tag{A3}$$

$$F_E = \sqrt{\beta BN^2 B_{sim}}\left(e_{EI}(t) + je_{EQ}(t)\right) \tag{A4}$$

Each e term is an independent identically distributed random sample taken from a Gaussian random number generator with unity variance. The two e terms for the spontaneous emission correspond to the in-phase "I" and quadrature "Q" components.

Table A1. Definition of laser parameters and their values used in the simulations.

Symbol	Definition	Value and/or Unit
N	Carrier density	m^{-3}
E	Laser field	$W^{0.5}$
I_{bias}	Laser bias current	13 to 33 mA
ΔI	Amplitude of gain-switching current	19 mA
e	Quantum of electronic charge	1.6×10^{-19} C
V	Volume of active region	3×10^{-17} m^3
A	Non-radiative carrier recombination rate coefficient	1×10^{9} s^{-1}
B	Bimolecular recombination rate coefficient	1×10^{-16} m^3 s^{-1}
C	Auger recombination rate coefficient	1×10^{-41} m^6 s^{-1}
a	Differential gain	7×10^{-13}
Γ	Confinement factor	0.3
ϵ_{nl}	Non-linear gain compression	1×10^{-23} m^3
α_H	Linewidth enhancement factor	4
N_0	Carrier density at transparency	1×10^{24} m^{-3}
τ_P	Photon lifetime	4 ps
β	Fraction of spontaneous emission into the lasing mode	1×10^{-5}
Δt	Simulation timestep	1 ps
B_{sim}	Simulation bandwidth [1]	1 THz

[1] Inverse of the simulation timestep.

For convenience, we take the PD current to be $|E|^2/(1 \times 10^{22})$ and a digital tenth-order Butterworth lowpass filter with a 3 dB bandwidth of twice the gain-switching modulation frequency is used to simulate bandwidth constraints in the entire system. To model the DI, we note that the numerical timestep is 1 ps;: the delay of the interferometer is 800 ps, which is importantly an integer number of the samples of the complex numerical array. The 800 ps DI is modeled by shifting the samples by 800 samples, multiplying by '*j*' where $j = \sqrt{-1}$ and adding the two arrays. An optimum sampling instance is found, and then, a histogram of the distribution of the DI output voltage is made.

References

1. Ma, X.; Yuan, X.; Cao, Z.; Qi, B.; Zhang, Z. Quantum random number generation. *NPJ Quantum Inf.* **2016**, *2*, 16021. [CrossRef]
2. Seyhan, K.; Akleylek, S. Classification of random number generator applications in IoT: A comprehensive taxonomy. *J. Inf. Secur. Appl.* **2022**, *71*, 103365. [CrossRef]
3. See for Example: Quantum Random Number Generation Applications. Available online: https://www.idquantique.com/random-number-generation/applications/ (accessed on 31 July 2023).
4. Tokunaga, C.; Blaauw, D.; Mudge, T. True Random Number Generator With a Metastability-Based Quality Control. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2008**, *43*, 78–85. [CrossRef]
5. Sunar, B.; Martin, W.J.; Stinson, D.R. A provably secure true random number generator with built-in tolerance to active attacks. *IEEE Trans. Comput.* **2007**, *56*, 109–119. [CrossRef]
6. Liu, Y.; Cheung, R.C.C.; Wong, H. A bias-bounded digital true random number generator architecture. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2017**, *64*, 133–144. [CrossRef]
7. Carreira, L.; Danielson, P.; Rahimi, A.; Luppe, M.; Gupta, S. Low-Latency Reconfigurable Entropy Random Number Generator with Bias Detection and Correction. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2020**, *67*, 1562–1575. [CrossRef]
8. Luo, Y.; Zhao, Y.; Li, J.; Çetintaş, E.; Rivenson, Y.; Jarrahi, M.; Ozcan, A. Computational imaging without a computer: Seeing through random diffusers at the speed of light. *eLight* **2022**, *2*, 4. [CrossRef]
9. Sciamanna, M.; Shore, K.A. Physics and applications of laser diode chaos. *Nat. Photon.* **2015**, *9*, 151–162. [CrossRef]
10. Chenye, Q.; Kunpeng, J.; Qianyuan, L.; Teng, T.; Xiaohan, W.; Yanhong, G.; Shu-Wei, H.; Yuan, L.; Shining, Z.; Zhenda, X.; et al. Electrically controllable laser frequency combs in graphene-fibre microresonators. *Light Sci. Appl.* **2020**, *9*, 185. [CrossRef]
11. Shen, B.; Shu, H.; Xie, W.; Chen, R.; Liu, Z.; Ge, Z.; Zhang, X.; Wang, Y.; Zhang, Y.; Cheng, B.; et al. Harnessing microcomb-based parallel chaos for random number generation and optical decision making. *Nat. Commun.* **2023**, *14*, 4590. [CrossRef]
12. Monet, F.; Boisvert, J.S.; Kashyap, R. A simple high-speed random number generator with minimal post processing using a random Raman fiber laser. *Sci. Rep.* **2021**, *11*, 13182. [CrossRef] [PubMed]
13. Bruynsteen, C.; Gehring, T.; Lupo, C.; Bauwelinck, J.; Yin, X. 100-Gbit/s Integrated Quantum Random Number Generator Based on Vacuum Fluctuations. *PRX Quantum* **2023**, *4*, 010330. [CrossRef]
14. Septriani, B.; de Vries, O.; Graefe, M. Quantum random number generation (QRNG) by phase diffusion process in a gain-switched semiconductor laser—New insights. In *CLEO: QELS_Fundamental Science*; Optica Publishing Group: San Jose, CA, USA, 2019; pp. 1–2.
15. Lovic, V.; Marangon, D.G.; Lucamarini, M.; Yuan, Z.; Shields, A.J. Characterizing Phase Noise in a Gain-Switched Laser Diode for Quantum Random-Number Generation. *Phys. Rev. Appl.* **2021**, *16*, 054012. [CrossRef]
16. Paraïso, T.K.; Roger, T.; Marangon, D.G.; De Marco, I.; Sanzaro, M.; Woodward, R.I.; Dynes, J.F.; Yuan, Z.; Shields, A.J. A photonic integrated quantum secure communication system. *Nat. Photon.* **2021**, *15*, 850–856. [CrossRef]
17. Quirce, A.; Valle, A. Random polarization switching in gain-switched VCSELs for quantum random number generation. *Opt. Expr.* **2022**, *30*, 10513–10527. [CrossRef]
18. Shakhovoy, R.; Sharoglazova, V.; Udaltsov, A.; Duplinskiy, A.; Kurochkin, V.; Kurochkin, Y. Influence of chirp, jitter, and relaxation oscillations on probabilistic properties of laser pulse interference. *IEEE Quantum Electron.* **2021**, *57*, 2000307. [CrossRef]
19. Ito, H.; Yokoyama, H.; Murata, S.; Inaba, H. Picosecond optical pulse generation from an r.f. modulated AlGaAs d.h. diode laser. *Electron. Lett.* **1979**, *15*, 738–740. [CrossRef]
20. Osinski, M.; Adams, M. Picosecond pulse analysis of gain-switched 1.55 μm InGaAsP laser. *IEEE J. Quantum Electron.* **1985**, *21*, 1929–1936. [CrossRef]
21. Gunning, P.; Lucek, J.K.; Moodie, D.G.; Smith, K.; Davey, R.P.; Chernikov, S.V.; Guy, M.J.; Taylor, J.R.; Siddiqui, A.S. Gainswitched DFB laser diode pulse source using continuous wave light injection for jitter suppression and an electroabsorption modulator for pedestal suppression. *Electron. Lett.* **1996**, *32*, 1010–1011. [CrossRef]
22. Anandarajah, P.M.; Maher, R.; Xu, Y.Q.; Latkowski, S.; O'Carroll, J.; Murdoch, S.G.; Phelan, R.; O'Gorman, J.; Barry, L.P. Generation of Coherent Multicarrier Signals by Gain Switching of Discrete Mode Lasers. *IEEE Photon. J.* **2011**, *3*, 112–122. [CrossRef]
23. Ó Duill, S.P.; Zhou, R.; Anandarajah, P.M.; Barry, L.P. Analytical approach to assess the impact of pulse-to-pulse phase coherence of optical frequency combs. *IEEE J. Quantum Electron.* **2015**, *51*, 1200208. [CrossRef]

24. Chrysostomidis, T.; Roumpos, I.; Alvarez Outerelo, D.; Troncoso-Costas, M.; Moskalenko, V.; Garcia-Escartin, J.C.; Diaz-Otero, F.J.; Vyrsokinos, K. Long term experimental verification of a single chip quantum random number generator fabricated on the InP platform. *EPJ Quantum Technol.* **2023**, *10*, 5. [CrossRef]
25. Rukhin, A.; Soto, J.; Nechvatal, J.; Smid, M.; Barker, E.; Leigh, S.; Levenson, M.; Vangel, M.; Banks, D.; Heckert, A.; et al. *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*; NIST Special Publication: Gaithersburg, MD, USA, 2010; Volume 800, p. 22.
26. Schunk, N.; Petermann, K. Noise analysis of injection-locked semiconductor injection lasers. *J. Quantum Electron.* **1986**, *22*, 642–650. [CrossRef]
27. O'Duill, S.P.; Barry, L.P. High-resolution simulation of externally injected lasers revealing a large regime of noise-induced chaos. *Photonics* **2022**, *9*, 83. [CrossRef]