Chrysostomidis et al. *EPJ Quantum Technology* (2023) 10:5
https://doi.org/10.1140/epjqt/s40507-023-00162-5

EPJ Quantum Technology
a SpringerOpen Journal

RESEARCH Open Access

Long term experimental verification of a single chip quantum random number generator fabricated on the InP platform

Themistoklis Chrysostomidis[1*], Ioannis Roumpos[1], David Alvarez Outerelo[2], Marcos Troncoso-Costas[3], Valentina Moskalenko[4], Juan Carlos Garcia-Escartin[5], Francisco J. Diaz-Otero[2] and Konstantinos Vyrsokinos[1]

*Correspondence: tchrysos@auth.gr
[1]School of Physics, Aristotle University of Thessaloniki, 54124, Thessaloniki, Greece
Full list of author information is available at the end of the article

Abstract

This work presents the results from the experimental evaluation of a quantum random number generator circuit over a period of 300 minutes based on a single chip fabricated on the InP platform. The circuit layout contains a gain switched laser diode (LD), followed by a balanced Mach Zehnder Interferometer for proper light power distribution to the two arms of an unbalanced MZI incorporating a 65.4 mm long spiral waveguide that translates the random phase fluctuations to power variations. The LD was gain-switched at 1.3 GHz and the chip delivered a min-entropy of 0.5875 per bit after removal of the classical noise, resulting a total aggregate bit rate of 6.11 Gbps. The recoded data set successfully passed the 15-battery test NIST statistical test suite for all data sets.

Keywords: Quantum random number generator; InP platform; Integrated optics; Integrated quantum devices

1 Introduction

Generation of random numbers at high speed is extremely valuable in a wide range of applications including quantum key distribution systems cryptography [1], stochastic modeling [2], Monte Carlo and numerical simulations [3, 4], extensive data processing [5], decision making algorithms [6], and lottery gambling [7, 8].

Although pseudo-random numbers are produced easily by computational techniques, randomness is considered "true" only if it is theoretically proven [9]. These true random numbers are generated only by physical processes like noise signal emitted by optical or electrical sources, free running oscillators, chaos, and quantum entropy sources [8], with the latter ones being a subclass of physical random number generators. These derive their unpredictability from quantum mechanical processes generated by a combination of quantum events [10].

Nowadays, quantum random number generators (QRNGs) are considered the best solution for generating true random numbers in cryptography and other applications that

require the highest credentials of randomness [8]. Towards this direction, several quantum sources have been investigated as QRNGs based on various phenomena such as a single photon taking two paths and its detection by single photon avalanche diode photodetectors [11, 12], the detection of amplified spontaneous emission (ASE) signals [13, 14], the measurement of the photon arrival time [15], vacuum state fluctuations [16], laser chaotic signals [17, 18], and, as in this work, the phase noise of laser diodes [19–26]. Among all the above schemes, QRNGs based on the phase noise in continuous-wave (CW) or pulsed semiconductor lasers, also mentioned as phase diffusion, provide remarkable simplicity, low-cost, high speed operation up to 43 Gbps [22], robustness and operation with flexible clock rate [21]. Phase noise QRNGs are based on the phase information of a semiconductor single mode laser's light output that contains a random component caused by the mixture of quantum phenomena, when it is operated near or below the lasing threshold [27], where the quantum noise dominates the phase fluctuations compared to the classical noise. Direct measurement of the random phase of optical signals is not physically viable, but the interference of two light signals with equal intensity and random phase difference produces amplitude fluctuated light [10], that can be received by a photodetector and digitized on an analog-to-digital converter (ADC) to generate raw random data. With proper post-processing in order to remove the bias from the classical noise contribution, these signals can be translated to true random numbers.

QRNGs based on phase noise on bulk and integrated devices have been demonstrated in various configurations exploiting the phase noise from semiconductor lasers. The simplest approach is by operating the laser with a low constant current near the threshold, where the quantum phase noise dominates over the classical one [24, 26]. If the delay between the two arms of an unbalanced Mach Zehnder Interferometer (uMZI) is way higher than the coherence time of the laser, the light's randomness can be extracted from the amplitude variation of the pulses at the uMZI output. The disadvantage of this method is the low intensity of the laser and the limited rate due to the coherence laser time. Another way to produce random numbers with higher rate is by driving a laser diode with a strong modulation current, well above and below threshold with sinusoidal or square pulses and connecting at its output an uMZI for the translation of the phase diffusion to pulses with a random variable peak power. This method measures the accelerated phase noise because the laser is below the threshold or even reversed bias for a long period of the pulse [23]. This type of QRNG's were originally shown with polarization-maintaining fiber based delayed interferometers [22, 23], but with the progress of photonic integration technology, the latest results are coming from Silicon photonics [28], and silicon on insulator (SOI) [29], platforms. A gain-switch (GS) mode laser is employed as a phase-diffusion quantum entropy source and coupled to a Si photonic chip that comprises the uMZI and the detection components [28], and achieves full entropy capacity around 820 Mbps. Recently, a 10 Gbps QRNG has been demonstrated [29], using a packaged on-chip tunable SOI critical interferometry structure for QRNGs based on phase diffusion laser operating in GS mode. A major problem though with Si photonics based devices is that the laser sources should be external, although hybrid integration of directly modulated lasers has been recently demonstrated [30]. The only mature platform that offers the intrinsic co-integration of active and passive devices in the C-band is InP. Following this path, a single InP chip quantum entropy QRNG source based on the interference of one GS and one CW laser is demonstrated in [31], where the chip also includes a high speed photodetector and the in-

terferometric coupler. The aggregate speed was relatively low, as the GS Laser Diode (LD) was modulated at 100 MHz, without providing any other details about the final QRNG bit rate. In the same rationale, a more advanced layout is proposed in [32], by replacing the CW LD with a second gain switched one, while adding also two variable attenuators on the two light paths for proper power adjustments before interference. The aggregate bit rate now is raised to 8 Gbps, but this setup requires doubling the RF injected power and precise synchronization of the two clock signals.

In this work we are presenting for the first time the results from a single chip QRNG circuit fabricated on the InP platform that is relying on cascading a gain switched LD followed by a delayed interferometer. The distributed Bragg reflector (DBR) laser of the proposed circuit is modulated at 1.3 GHz followed by an uMZI of 65.4 mm differential delay for the generation of true random numbers at 6.11 Gbps. The same chip also includes a tunable coupler in the form of a balanced MZI (bMZI) for directing the proper power to the path with the longest waveguide of the uMZI and a photodiode (PD) for optical to electrical conversion towards demonstrating a single photonic integrated circuit (PIC) high speed QRNG, easily embedded in large systems. However, this on-chip PD was not included in the measurements presented in this article due to the high electrical crosstalk, between the high-power RF signal driving the diode and the low power signal reaching the PD. This fact has not prevented the further evaluation of the circuit with an external PD. The performance and the stability of the QRNG was tested by recording 12 streams of 12.5 μs and 14 streams of 125 μs in a time frame of 300 minutes at 80 GS/s, with results from the raw data revealing a 5.719 mean value of the min-entropy out of 8 bits from the ADC for all 26 files with a standard deviation (1σ) of 0.0532 bits. After removal of the classical noise, these values were reduced to 4.775 and 1σ of 0.0310, respectively, confirming the hight stability of the PIC operation. A post processing Toeplitz hashing randomness extractor with 0.5785 reduction factor (4.7/8) was applied offline on each data set to distill the randomness. The hashed data were tested afterwards using the 15-battery test NIST statistical test suite, where all applicable tests were passed, verifying in this way the capability of true random generation of the proposed device over a long period of time. The randomness of the data was verified also by calculating the autocorrelation coefficient for one 12.5 μs and 125 μs file revealing values below 10^{-2} and 3×10^{-3}, respectively after post-processing with the Toeplitz extractor. The presented quantum random number generator PIC is another step towards the minimization of quantum circuits for integration with existing systems that will pave the way for commercialization of this technology in existing or new applications.

2 Methods

2.1 PIC description and principle of operation

The PIC was fabricated via Smart Photonics foundry services offering the InP active-passive co-integration platform. Figure 1(a) shows a top view photo of the monolithically integrated chip with a total footprint 9 mm^2, and Fig. 1(b) depicts a schematic layout of the QRNG circuit featuring two DBR lasers, one 3×3 and two 2×2 MMI couplers, all with equal splitting ratio, two electro-optic (EO) phase shifters, one on-chip PD and a spiral waveguide 65.4 mm long. The two DBR lasers, together with an external input port, are connected to the 3×3 multi-mode interferometer (MMI), with two out of the three output ports connected to the two electro-optic phase shifters, followed by the first 2×2

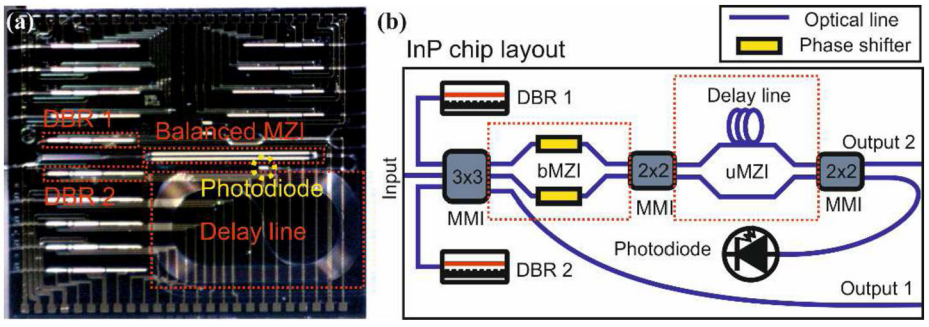

Figure 1 (**a**) Top-view photo of the QRNG monolithic integrated InP chip. (**b**) Chip layout of the QRNG section. DBR: distributed Bragg reflector laser, MMI: Multimode interferometer, u/bMZI: unbalanced/balanced Mach-Zehnder interferometer

MMI coupler. In this way a bMZI is formed acting as a tunable coupler that can control the power distribution at the two output ports. The third port is guided to the edge of the chip, Output 1 in Fig. 1(b), for fiber to chip alignment and independent characterization of the DBR lasers. The output ports of the first 2×2 MMI are connected through the short and the long spiral waveguides to the second 2×2 MMI, forming in this way the uMZI, where the phase diffusion from the laser is translated to amplitude modulation. The propagation losses at the spiral, according to the process design kit (PDK), are 3 dB/cm for a total estimated loss of 19.6 dB. The insertion loss per 2×2 MMI coupler is 0.5 dB with a maximum imbalance of 0.5 dB. The second output from the uMZI is guided to an on-chip PD with 18 GHz 3 dB EO bandwidth that was targeted to demonstrate the full on-chip QRNG operation from the PIC. However, the high power injected to the GS laser in combination with the low power of the signal reaching the PD resulted in heavy electrical crosstalk that prevented any meaningful detection of the pulsed signal at the oscilloscope. For this reason, the evaluation of the InP chip was carried out through Output 2 that is connected to the first output of the uMZI.

The principle of operation for this QRNG is based on gain switching one out of the two DBR lasers by setting the bias slightly below the threshold, while applying a strong electrical sinusoidal signal forcing its operation at below/above threshold states between the injected electrical pulses. Below threshold, strong attenuation occurs at the cavity field and spontaneous emission dominates the cavity. This attenuates any prior phase coherence, while the spontaneous emission produces a masking field with a true random phase. Above threshold, the cavity field is rapidly amplified to a macroscopic level due to gain saturation, resulting in a random phase but a predictable amplitude of the field. The periodic operation around threshold results in a stream of phase-randomized, nearly identical optical pulses [23]. The amplification is electrically pumped and is phase-independent, so the phase of the cavity field remains truly random. The interference of subsequent pulses with random phase leads to the formation of pulses with random amplitude. The translation of the peak power of the pulses at the output of the uMZI with a photodetector and an ADC leads to binary random generation. In the PIC tested here, the 65.4 mm long spiral introduces a 770 ps delay that enables stable interference when the laser is gain switched at 1.3 GHz. The bMZI helps maximize the contrast of the interference, by sending the maximum possible optical power to the path of the uMZI with the spiral for compensating the extra propagation losses.

2.2 On-chip component characterization

Figure 2 presents the P-I curves and the optical spectra from the static characterization of DBR 1 and DBR 2 lasers, both recorded at Output 1 of the chip with a single mode fiber. From this graph the threshold values of DBR 1 and DBR 2 are identified as 21 mA and 10 mA, respectively. Also, the spectra from the operation of the lasers close to the threshold reveals a single mode response with the side mode suppression ratio (SMSR) measured as 33 dB for DBR 1 and 38 dB for DBR2 at 21 mA and 13 mA respectively. As DBR 2 exhibited lower threshold current and better SMSR, it was decided to proceed to further evaluation of the chip with this laser source. The optical power measured from this LD with a power meter at Output 1 for 10 mA and 13 mA, slightly above the threshold, was −39 and −31.8 dBm, respectively.

The dynamic characterization of the DBR laser was performed via mixing a DC voltage from a power supply and an RF signal from a signal generator through a Bias-T with 12.5 GHz bandwidth. The mix of the DC and RF signals was applied to the laser via a GSG RF probe tip with 18 GHz bandwidth. By operating the laser with variable DC and RF voltages, the GS operation of the laser was recorded at Output 1 for two different biasing conditions. Figure 3(a) shows the eye diagram of the pulses for 18 mA bias and 20 dBm for the RF sinusoidal wave, while Fig. 3(b) illustrates the eye diagram when the laser is biased at 33 mA with 25 dBm RF power. Figure 3(a) shows that when the laser is biased around the threshold, there is a strong fluctuation of the power of the pulses, a fact that also affects the distribution of the pulses emerging after the contrast interference of the uMZI, as will be shown later. The temperature of the chip was controlled by placing the chip on top of a vacuum chuck featuring a temperature control ensuring stable conditions at 23°C. Since the output power coming from the chip was very low due to low biasing conditions of the laser and the high path losses from the spiral, at the output of the chip it was placed a low noise erbium doped fiber amplifier (EDFA), followed by an optical bandpass filter (OBPF) with 1 nm bandwidth for out of band noise rejection. The

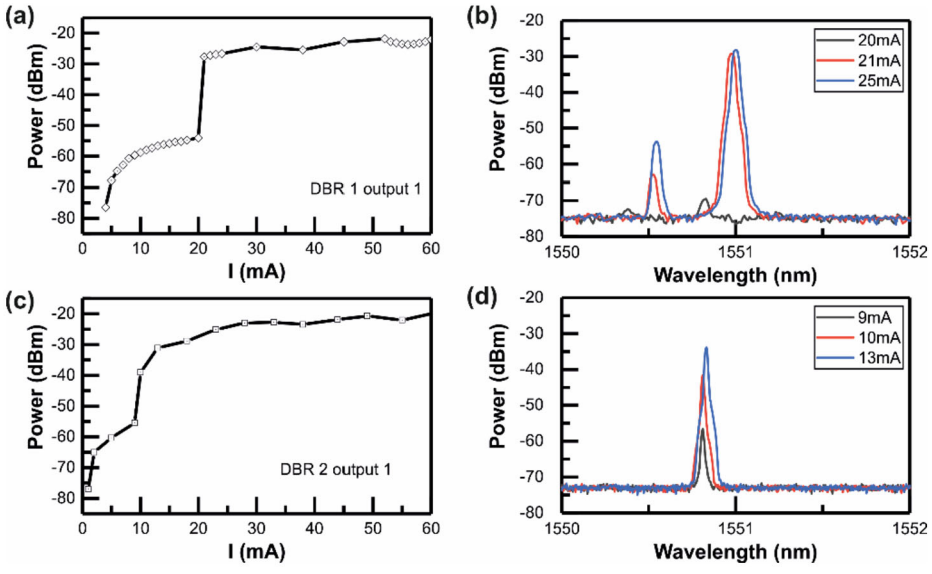

Figure 2 (**a**) DBR laser 1 P-I curve measured at Output 1 and (**b**) the spectrum of laser emission near threshold. (**c**) DBR laser 2 P-curve measured at Output 2 and (**d**) the spectrum of laser emission near threshold

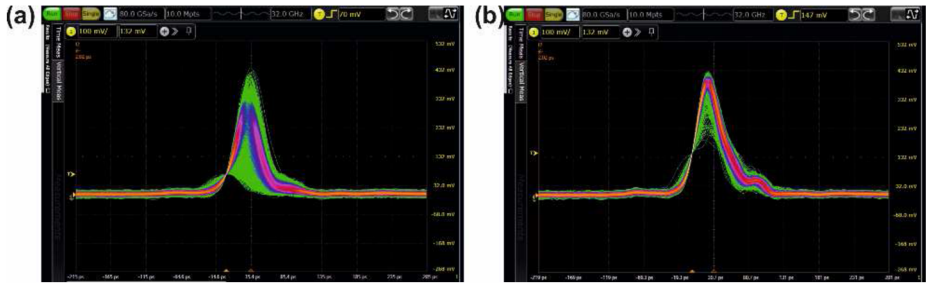

Figure 3 Amplitude fluctuation of the GS operation (**a**) DC bias near threshold, I = 18 mA, (**b**) DC bias above threshold, I = 33 mA

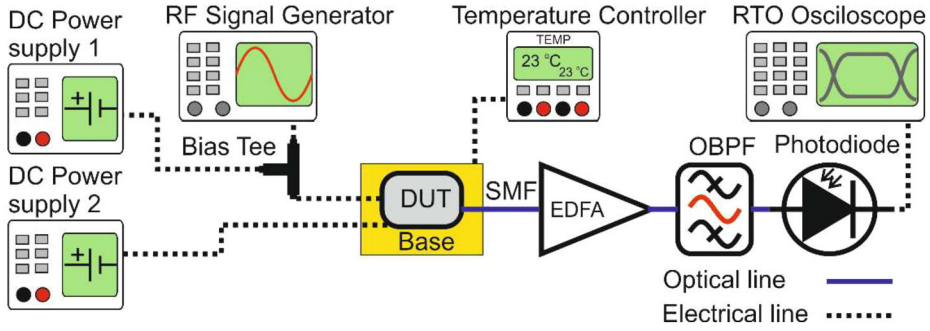

Figure 4 Experimental set up for the PIC components characterization and QRNG evaluation. DUT: Device Under Test, SMF: Single Mode Fiber, EDFA: Erbium Doped Fiber Amplifier, OBPF: Optical Bandpass Filter, RTO: Real Time Oscilloscope

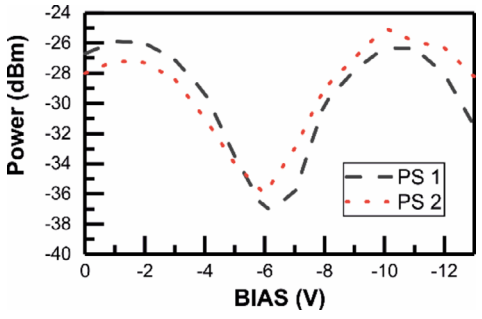

Figure 5 Power measured at output 2 for different BIAS voltage at balanced MZI upper (dash) and lower branch (dot)

amplified signal was then injected into a 70 GHz bandwidth PD connected to a real time oscilloscope (RTO) with 33 GHz bandwidth and 80 GSa/s sampling rate. Figure 4 shows the layout of the experimental setup.

The performance of the bMZI was evaluated by injecting light from Input (Fig. 1(b)) with an external CW laser operating at 1550 nm with 10 dBm power and collecting it from Output 2. Figure 5 shows the corresponding results when DC voltage is applied on the upper and lower phase shifter of the bMZI. The highest/lowest power is measured when the bMZI sends the most power over the short/long arm of the uMZI. It should be

noted that the two PSs exhibit similar performance with a V_π of 4 V, in agreement with the PDK of the foundry, and an extinction ratio of ∼12 dB. Given that the losses from the spiral are estimated at 19.6 dB, there is at least 7.6 dB power difference in the power of the two pulses colliding at MMI 2, resulting in significant degradation of the interference's contrast. It should be mentioned that Fig. 5 presents the combined response of the bMZI and uMZI for this wavelength.

2.3 Quantum random signal generation

After the characterization of the DBR lasers and the bMZI, the next step was the evaluation of the random generation capabilities of the circuit with the experimental setup illustrated in Fig. 4. The mixed signal driving the laser for the GS was a DC component with 1.1 V drawing 15 mA current from DC Power supply 1 and the sinusoidal RF component at 1.3 GHz with 15 dBm power. The insertion losses of the Bias-T and of the cable were 1 dB and 0.2 dB, respectively at this frequency, so the maximum RF power injected into the pads of the laser was 13.8 dBm. This value corresponds to 3.1 V_{pp} or 62 mA_{pp} modulation current, considering a 50 Ohm load resistance. However, in the GHz modulation range, the emerging effects of parasitic impedances of the LD and the circuit most likely reduce the actual current reaching into the LD active layer.

The best conditions in terms of contrast of interference were observed for –5.7 V at PS1. Then at Output 2 of the chip, the total collected power of the signal was –40 dBm. The receiver part is identical to the one described previously for the characterization of the GS operation of the laser. The 8-bit digital to analog converter (DAC) RTO display range was set to include the highest and lowest voltage value of the captured waveform coming from the chip. While keeping all applied signals to the chip constant, 12 waveforms of 12.5 μs duration and 14 waveforms of 125 μs were captured in regular intervals for a total time duration of 300 minutes. The different waveform durations were chosen to check if the duration has any effect on the pattern biases. In this way, the randomness performance of the PIC could be evaluated over an extended period and identify if there is any correlation between the peak power of the pulses. The temperature of the vacuum chuck was set at 23°C for the whole duration of the experiment to maintain stable operation condition on the tunable interferometer and the laser.

3 Results and discussion

3.1 Randomness quality evaluation

On each captured waveform a peak detection process was carried out by selecting the highest value in decimal form [Volts] of the peak, corresponding to an interference between two subsequent pulses in the uMZI. For the files with 12.5 μs duration, 162,500 peaks were detected, while for the 125 μs waveforms, the corresponding value was 1,625,000 corresponding to a 769.23 ps mean duration between peaks. The voltage display range at the RTO was 400 mV in the range [–33 mV, 367 mV], so with the 8-bit resolution the spacing of the 256 bins was 1.5625 mV. The lowest 32 bins in the files with a maximum voltage of 17.1875 mV is considered to be noise coming from the combination of the laser when it is below threshold, the EDFA and the noise of the ADC.

Figure 6(a) shows the distribution of the peak power of the first 125 μs data file, recorded at the output of the PIC for the conditions described above. The bin frequency profiles of the other 25 files exhibited almost identical profiles with a single peak of max value in the

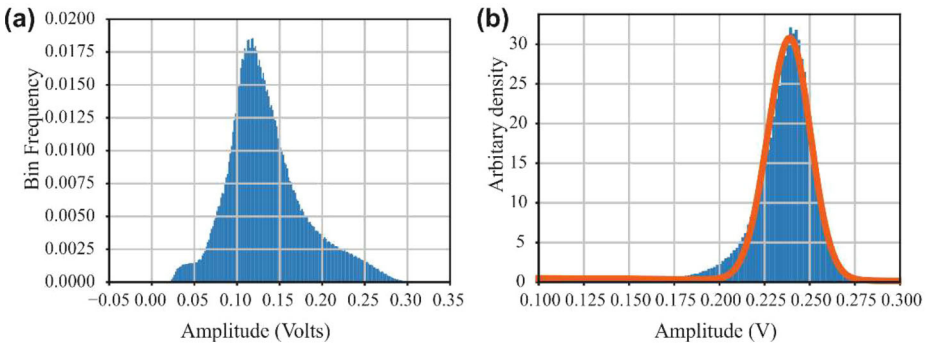

Figure 6 (**a**) Bin Frequency vs. peak power in Volts for the first 125 μs file at the output of the uMZI, (**b**) Peak power Intensity variation of GS pulses at output 1, the orange dot line illustrates the corresponding Gaussian distribution fitting

range of [0.0183–0.0210]. The profile of Fig. 6(a) though comes in contrast to the expected arcsine shape with the two peaks reported in other similar phase diffusion QRNG layouts [22, 23, 29]. To identify the reason for this discrepancy, the next step was the formation of a simplified model following the well-known interference equation:

$$I = I_1 + I_2 + 2\mathrm{VIS}\sqrt{I_1 I_2}\cos(\Delta\varphi + \varphi_o), \tag{1}$$

where I_1 and I_2 are the peak power of the colliding pulses, VIS is the visibility of the interferometer for our pulses and φ_o is the static phase difference due to the different light paths at the uMZI. The term $\Delta\varphi$ is the relative phase between successive pulses imposed by the GS operation and is assumed to follow a Gaussian distribution [33, 34].

The usual arcsine profile that appears in other QRNG demonstrators based on the random phase of independent pulses appears when the Gaussian phase is wide enough to be, for all practical purposes, a uniform random variable between 0 and 2π [22, 23, 29]. For continuous wave lasers, the Gaussian phase drift depends on the delay between the interfering signals, but usually has a smaller variance [26, 31]. In the gain switching operation of our system, the Gaussian phase drift is related to the modulation current. While there is no simple closed formula, the phase remains a Gaussian random variable and the variance can be determined empirically from experimental measurements [34]. After obtaining the histogram of the output voltages from the experimental data, we have found the best fit for the unknown parameters in Equation (1).

The profile of intensity I_1 was extracted by recording at Output 1 the GS pulses directly from the laser. Figure 6(b) shows the distribution of the peak power of the pulses extracted by the data file and reveals a Gaussian distribution with $R^2 = 0.985$ of 0.238 V mean value and 1σ of 0.0118. For I_2, it was assumed that the pulses' peak power follows the same Gaussian distribution with a mean value that was divided by a factor of six in the linear scale, corresponding to the uncompensated 7.6 dB extra losses from the uMZI spiral. The 1σ was set equal to 0.002. The three unknown parameters were thus the VIS, the φ_o and the $\Delta\varphi$.

Figure 7 shows a narrow set of results from the simulations for VIS values of 0.8, 0.6 and 0.4, $\Delta\varphi$ of 1σ equal to 30°, 60° and 90° and a φ_o that is variable between 0° and 360°. For $\Delta\varphi$ higher than 90°, the result is always a two peak bin distribution that does not match

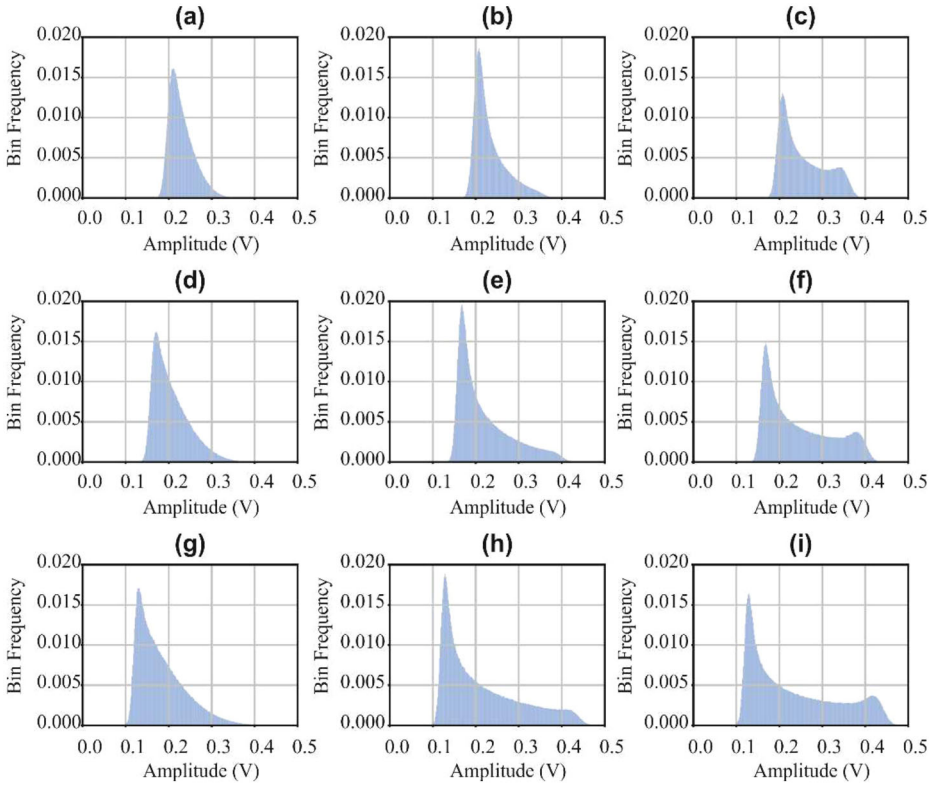

Figure 7 Bit Frequency vs. peak power in Volts for variable VIS, $\Delta\varphi$ and φ_o conditions for the PIC under investigation (**a**) VIS = 0.4, $\Delta\varphi = 30°$ and $\varphi_o = 135°$, (**b**) VIS = 0.4, $\Delta\varphi = 60°$ and $\varphi_o = 180°$, (**c**) VIS = 0.4, $\Delta\varphi = 90°$ and $\varphi_o = 195°$, (**d**) VIS = 0.6, $\Delta\varphi = 30°$ and $\varphi_o = 135°$, (**e**) VIS = 0.6, $\Delta\varphi = 60°$ and $\varphi_o = 150°$, (**f**) VIS = 0.6, $\Delta\varphi = 90°$ and $\varphi_o = 195°$, (**g**) VIS = 0.8, $\Delta\varphi = 30°$ and $\varphi_o = 135°$, (**h**) VIS = 0.8, $\Delta\varphi = 60°$ and $\varphi_o = 135°$, (**i**) VIS = 0.8, $\Delta\varphi = 90°$ and $\varphi_o = 195°$

the experimental results and thus were discarded from further evaluation. The parameter φ_o of Fig. 7 is selected to show only graphs featuring a single peak with max frequency bin of 0.0175–0.02 for agreement with Fig. 6(a) and the other 26 data files. As it is clear the best fit comes for VIS = 0.6, $\Delta\varphi = 60°$ and $\varphi_o = 150°$, where the bin range is a little bit over 0.313 V. The difference in the x-axis range is coming from the fact that the mean power of the pulses in the simplified model is higher than the actual ones interfering at the output coupler, as the losses of the bMZI and the PIC-fiber interface were not considered in the model. The deviations for perfect matching between Fig. 6(a) and Fig. 7(e) are related to the consideration of a perfect laser for the light pulse generation, ignoring all physics related to operating the diode at high-speed operation close to its threshold and the dynamic effects emerging in these conditions [31, 34, 35].

The next step after the simplified phase diffusion calculation was to evaluate the randomness quality of the output signal initially through its entropy calculation. Based on the results for the measurement depicted in Fig. 6(a), the min-entropy is calculated equal to 5.75 per 8 bits of the ADC, using the well-known formula:

$$H_{\min} = -\log_2(p_{\max}), \tag{2}$$

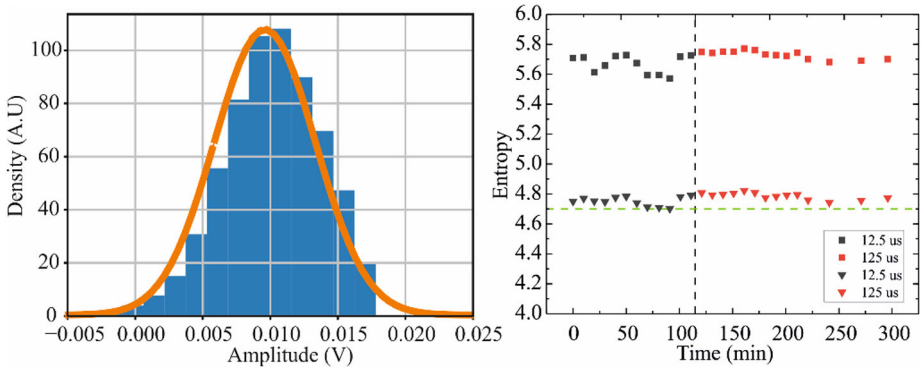

Figure 8 (**a**) Histogram of classical noise between peaks for the first 125 μs file with the orange line illustrating the Gaussian fit, (**b**) min entropy values for all 26 files including classical noise (square) and after the removal of the Gaussian noise (triangle)

where ($p_{\max}$) is the probability of the most likely event, that is equal to 0.0185. However, this value refers to total randomness, including the classical Gaussian noise sources of the system. For enhanced security, the QRNG should be free of the classical noise influence. To estimate the effect of this noise, we studied the measured voltages when there was no laser pulses. Figure 8(a) presents the histogram of the power distribution of the 32 lower power bins for the same file as in Fig. 6(a). The density of the noise bins can be approximated well with a Gaussian distribution of $R^2 > 0.99$ with a mean value of 9.59 mV and 1σ of 3.739 mV. As a heuristic, considering the maximum voltage noise level is not exceeded 98% of the time under the control of an external attacker and assuming a worst-case scenario where the attacker can assign to each bin the counts corresponding to the neighboring voltages within the range of this noise voltage, the min-entropy is recalculated to 4.78 per 8 bits [34] after removing the noise from the ADC of the RTO, the noise from the EDFA and the noise from the laser under threshold conditions. However, the second and third components are mostly of quantum origin and have been used before for quantum random number generation [13, 14, 36–38]. Therefore, it is expected that the actual min-entropy should be higher than this. Indeed, by assuming that the classic noise from the ADC according to the datasheet of the RTO for the recording conditions in the experiment is 2 mV, the maximum min-entropy is 5.49 per 8 bits in a rather optimistic calculation. In a well isolated chip where the signal can be collected with the on-chip photodetector without the EDFA, the min-entropy could be calculated by models for quantum entropy coming solely from phase diffusion [33, 34]. The same concept was also applied for the other 25 files and Fig. 8(b) shows the corresponding results illustrating the min-entropy and min-entropy after subtraction of the classical noise. The mean value entropy is 4.775 with a 1σ of only 0.031 confirming the high stability of the InP QRNG PIC. The minimum value of the entropy is 4.7 for files 9–12 and is considered for the subsequent hashing of the raw data.

The estimation of the Gaussian noise free min-entropy value allowed the use of an entropy extraction process on the eight-bit binary conversion of the peak power of the pulses. The information-theoretically provable randomness extractor Toeplitz [9] was employed with extraction efficiency of 4.7 bits per peak sample. After these calculations, it is determined that the chip is capable of generating random numbers at the bit rate of 6.11 Gbps.

3.2 NIST statistical test suite and autocorrelation coefficient evaluation

The high entropy, homogeneous sequences obtained from the randomness extraction process were stacked into two groups of data sets; group A of all 12.5 μs files and group B of all 125 μs files for randomness evaluation with the 15-test battery test suite proposed by NIST [39]. The significance level was set to 10^{-2}, meaning that 1 out of 100 sequences is expected to fail the test even if it is produced by a completely random generator. Following the NIST test suite suggestions, the proportion defined as passed test/total tests and the uniformity of the P-values are computed and compared to their acceptance limit. As shown in Fig. 9 all the applicable tests are passed for 100 bitstreams of 91k and 1M length, corresponding to group A and group B data sets, respectively. From the comparison of the test results between group A and B, it is concluded that the difference in the waveform duration does not hide or reveal any pattern bias. The minimum proportion pass rate for each statistical test, with the exception of the random excursion/variant test, is approximately 0.96. The random excursion/variant minimum pass rate is 0.944 as indicated with the red vertical lines. It is important to also note that for Fig. 9(a–b) the Mauer's universal test requires a bit stream of 1 M length to compute the statistic and therefore it is not possible to determine if group A passes or fails on this assignment. The NIST statistical tests reveal that the obtained results show a high probability of randomness for the recorded sequence incorporating all 26 files over the 300 minute time period.

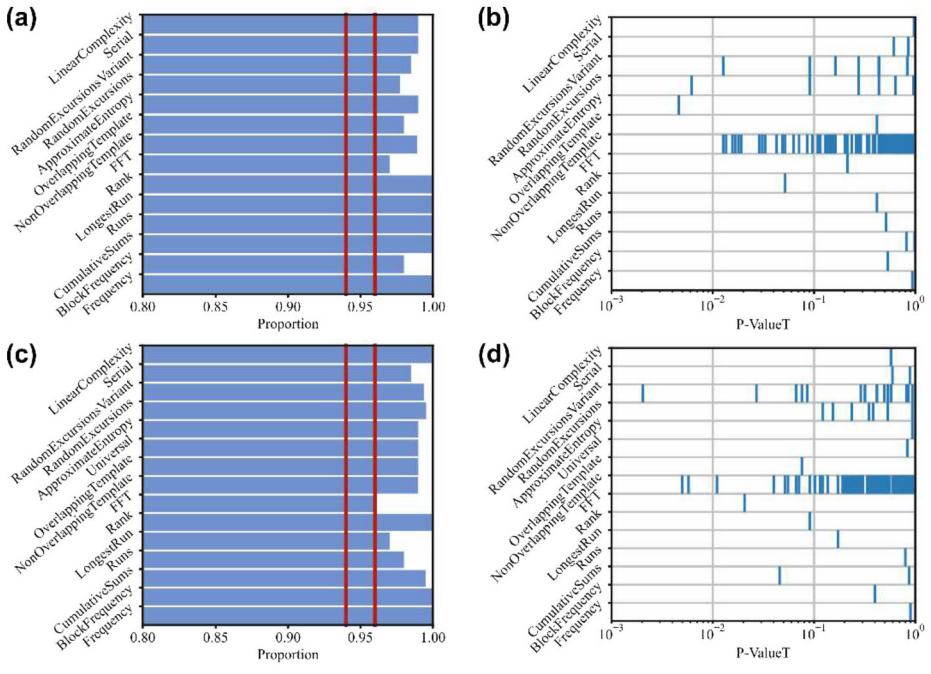

Figure 9 Summary of the NIST test suite results. (**a**), (**c**) The minimum proportion pass rate of the 10^{-2} confidence interval for each statistical test, with exception of the random excursion/variant test, is approximately 0.96 for a sample size of 100 binary sequences with a bitstream length of 91K and 1M, the random excursion/variant minimum pass rate is 0.944 as indicated with the red vertical lines. For the tests with multiple outcomes like the non-overlapping template (NOT) the proportion area is averaged. (**b**), (**d**) To ensure the distribution of P-values is uniform, a chi-square test was applied to determine a P-valueT corresponding to the Goodness-of-Fit distributional Test on the p-values obtained for each test, with PvalueT = $\Gamma(9/2, \chi\, 2/2)$ for each test and its subtests is calculated. For all test the PvalueT > 10^{-4} (sequence can be considered uniformly distributed)

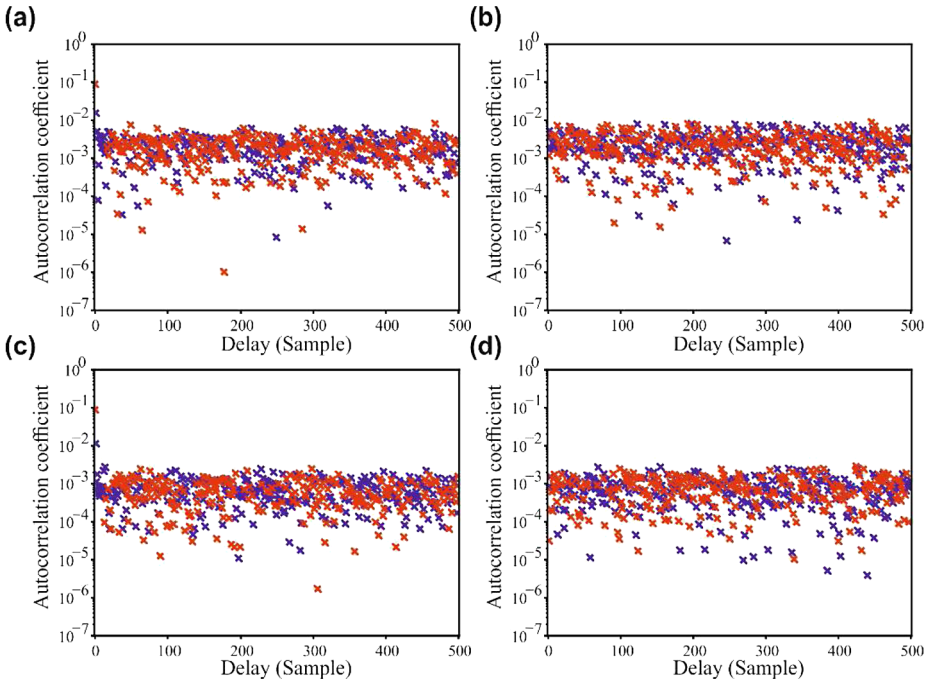

Figure 10 Autocorrelation coefficient for the last 12.5 μs file (**a**) before and (**b**) after post-processing with the Toeplitz extractor, (**c**) Autocorrelation coefficient for the last 125 μs file and (**d**) same file after post-processing with the Toeplitz extractor

The randomness of the data was verified also by calculating the autocorrelation coefficient for up to 500 samples for all data files. Figure 10 shows the corresponding results for the last of the twelve 12.5 μs and 125 μs files, before and after post processing with the Toeplitz extractor. For both file size, the raw data for delay 1 and 2 exhibit a coefficient in the order of 10^{-1} and 10^{-2} respectively that originates from the non-ideal estimated $\sim 0.33\pi$ 1σ phase diffusion during gain switching of the laser. However, after hashing the coefficient is reduced to below 10^{-2} for all delay values confirming the randomness of the generated data. Also, it is important to note that for the 125 μs files, the autocorrelation after hashing is now below 3×10^{-3}. Similar response weas observe also for the other twenty-four files and therefore are omitted from the manuscript.

3.3 Proposed circuit performance enhancement

The overall performance of the QRNG PIC could be significantly improved by shortening the spiral length at the uMZI, as this would reduce the overall losses and simultaneously increase the aggregate bit rate. It should be mentioned just for reference that the LD was successfully gain switched at 10 GHz when biased at high currents. A faster pulse rate would allow a shorter delay assuming random phase diffusion in between subsequent pulses is still valid in these rates. In addition, it would also improve the contrast of the interfering pulses, as the two branches would possess equal power. Furthermore, better electrical isolation of the PD would enable single chip QRNG operation, which was the initial target of the layout design. In terms of operation conditions, by replacing the signal generator with a pulse pattern generator, the LD would produce almost squared pulses, which would drastically improve the contrast of the interference, as there is higher toler-

ance to temporal pulse misalignments. Also, by selecting the part of the pulses with the steady-state emission for interference, we could eliminate the effect of the random time jitter introduced by the spontaneous emission on the switch-on time of the laser [21], and would also minimize the frequency chirping that occurs due to the violent change in the carrier density [32].

4 Conclusions

In conclusion this work demonstrates for the first time a single PIC on the InP platform for high speed quantum random number generation based on the phase diffusion of GS laser source and a delayed interferometry structure. The chip contains two DBR lasers capable of optical pulse generating at multi-GHz rate, an uMZI with a 65.4 mm long spiral waveguide in one arm, a tunable coupler in the form of a bMZI featuring EO phase shifters that adjust the incoming power to the two branches of the uMZI and a high speed PD. However, the PD was not employed in the experimental results of this article due to poor electrical isolation that prevented clear signal reception. By using an external PD, successful QRNG pulse sequences were recorded by gain switching one of the two LDs at 1.3 GHz over a period of 300 minutes. In total 12 files of 12.5 μs and 14 files of 125 μs were captured. A simplified model revealed that by comparing the bin count vs. the peak power with the experimental data from these files, the LD produced pulses with 1σ phase variation close to 60°, while the visibility of the interferometer was 0.6. The further processing of the raw data for all 26 files showed a 5.71 value for the min-entropy out of the 8-bit ADC of the RTO with a 1σ of 0.053. Subtracting the classical noise from the system so that we only keep the quantum contribution on the entropy reduced the mean value of the min-entropy to 4.77 with a 1σ of 0.031 confirming the high stability of the PIC operation over the extended 300 minutes period. For complete randomness characterization a Toeplitz randomness extractor was employed afterwards to the raw data to distill true random numbers using the estimated min-entropy of 4.7 per 8 bits. The confirmation of the high randomness of the signal from the InP PIC was demonstrated by testing the hashed data in the 15-battery test NIST statistical suite, where all applicable tests were passed with confidence. The calculation of the autocorrelation coefficient of the raw data revealed values below 10^{-2} and 3×10^{-3} for the 12.5 μs and 125 μs files, respectively after post-processing with the Toeplitz extractor. Further improvement in the performance of the PIC could be obtained by shortening the spiral at the uMZI and driving the LD with square pulses as to select only interference from the steady state operation of the pulses with decreased timing jitter and minimum frequency chirp. The presented integrated quantum random number generator circuit is another step towards the full integration of quantum devices, providing compatibility with existing systems that will pave the way for industrial and commercial applications of quantum technologies.

Acknowledgements

This work was supported by EU H2020 projects NEBULA (Contract Number 871658). We would also like to acknowledge Mr. Panagiotis Triantafullou for the custom mechanical items of the experimental setup. J.C. Garcia-Escartin has been funded by Ministerio de Ciencia e Innovación grant number PID2020-119418GB-I00 and by the Regional Government of Castilla y León (Junta de Castilla y León) and the EU-FEDER (CL-EI-2021-07, UIC 105).

Funding

Not applicable.

Availability of data and materials
The datasets used and/or analysed during the current study are available from the corresponding author on reasonable request.

Declarations

Competing interests
The authors declare no competing interests.

Author contributions
T.C and I.R performed the experimental work. V.M, D.A-O and F.D-O designed the integrated circuit. T.C, I.R, J.G-E and M.T-C completed the post processing. All authors analyzed and interpreted the results. T.C and K.V carried out the writing of the manuscript. All authors reviewed and approved the final manuscript.

Author details
[1]School of Physics, Aristotle University of Thessaloniki, 54124, Thessaloniki, Greece. [2]atlanTTic Research Center, University of Vigo, El Telecommunication, Campus Universitario s/n, 36310 Vigo, Spain. [3]School of Electronic Engineering, Dublin City University, Glasnevin, Dublin 9, Ireland. [4]Keysight Technologies, Santa Clara, CA, USA. [5]Dpto. Teoría de la Señal y Comunicaciones e Ingeniería Telemática, University of Valladolid, Campus Miguel Delibes, Paseo Belén n°15, 47011, Valladolid, Spain.

Publisher's Note

Received: 30 November 2022 Accepted: 7 February 2023 Published online: 10 February 2023

References
1. Scarani V, Bechmann-Pasquinucci H, Cerf NJ, Du M, Lütkenhaus N, Peev M. The security of practical quantum key distribution. Rev Mod Phys. 2009;81:1301–50. https://doi.org/10.1103/RevModPhys.81.1301.
2. Mascagni M, Qiu Y, Hin L-Y. High performance computing in quantitative finance: a review from the pseudo-random number generator perspective. Monte Carlo Methods Appl. 2014;20:101–20. https://doi.org/10.1515/mcma-2013-0020.
3. Cai X, Wang X. Stochastic modeling and simulation of gene networks—a review of the state-of-the-art research on stochastic simulations. IEEE Signal Process Mag. 2007;24:27–36. https://doi.org/10.1109/MSP.2007.273051.
4. Click T, Liu A, Kaminski G. Quality of random number generators significantly affects results of Monte Carlo simulations for organic and biological systems. J Comput Chem. 2011;32:513–24. https://doi.org/10.1002/jcc.21638.
5. Brin S, Page L. The anatomy of a large-scale hypertextual web search engine. Comput Netw ISDN Syst. 1998;30:107–17. https://doi.org/10.1016/S0169-7552(98)00110-X.
6. Shannon CE. Communication theory of secrecy systems. Bell Syst Tech J. 1949;28:656–715. https://doi.org/10.1002/j.1538-7305.1949.tb00928.x.
7. Hall C, Schneier B. Remote electronic gambling. In: Proc. 13th annu. comput. secur. appl. conf. 1997. p. 232–8.
8. Stipčević M, Koç Ç. True random number generators. 2014.
9. Ma X, Xu F, Xu H, Tan X, Qi B, Lo H-K. Postprocessing for quantum random-number generators: entropy evaluation and randomness extraction. Phys Rev A. 2013;87:62327. https://doi.org/10.1103/PhysRevA.87.062327.
10. Herrero-Collantes M, Garcia-Escartin JC. Quantum random number generators. Rev Mod Phys. 2017;89:15004. https://doi.org/10.1103/RevModPhys.89.015004.
11. Rarity JG, Owens PCM, Tapster PR. Quantum random-number generation and key sharing. J Mod Opt. 1994;41:2435–44. https://doi.org/10.1080/09500349414552281.
12. Jennewein T, Achleitner U, Weihs G, Weinfurter H, Zeilinger A. A fast and compact quantum random number generator. Rev Sci Instrum. 2000;71:1675–80. https://doi.org/10.1063/1.1150518.
13. Argyris A, Pikasis E, Deligiannidis S, Syvridis D. Sub-Tb/s physical random bit generators based on direct detection of amplified spontaneous emission signals. J Lightwave Technol. 2012;30:1329–34. https://doi.org/10.1109/JLT.2012.2188377.
14. Williams CRS, Salevan JC, Li X, Roy R, Murphy TE. Fast physical random number generator using amplified spontaneous emission. Opt Express. 2010;18:23584–97. https://doi.org/10.1364/OE.18.023584.
15. Wahl M, Leifgen M, Berlin M, Rohlicke T, Rahn H-J, Benson O. An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements. Appl Phys Lett. 2011;98:171105. https://doi.org/10.1063/1.3578456.
16. Gabriel C, Wittmann C, Sych D, Dong R, Mauerer W, Andersen U, Marquardt C, Leuchs G. A generator for unique quantum random numbers based on vacuum states. Nat Photonics. 2010;4:711–5. https://doi.org/10.1038/nphoton.2010.197.
17. Argyris A, Deligiannidis S, Pikasis E, Bogris A, Syvridis D. Implementation of 140 Gb/s true random bit generator based on a chaotic photonic integrated circuit. Opt Express. 2010;18:18763–8. https://doi.org/10.1364/OE.18.018763.
18. Ugajin K, Terashima Y, Iwakawa K, Uchida A, Harayama T, Yoshimura K, Inubushi M. Real-time fast physical random number generator with a photonic integrated circuit. Opt Express. 2017;25:6511. https://doi.org/10.1364/OE.25.006511.
19. Nie Y-Q, Huang L, Liu Y, Payne F, Zhang J, Pan J-W. The generation of 68 Gbps quantum random number by measuring laser phase fluctuations. Rev Sci Instrum. 2015;86:063105. https://doi.org/10.1063/1.4922417.
20. Raffaelli F, Sibson P, Kennard J, Mahler D, Thompson M, Matthews J. Generation of random numbers by measuring phase fluctuations from a laser diode with a silicon-on-insulator chip. Opt Express. 2018;26:19730. https://doi.org/10.1364/OE.26.019730.

21. Yuan Z, Lucamarini M, Dynes J, Frohlich B, Plews A, Shields A. Robust random number generation using steady-state emission of gain-switched laser diodes. Appl Phys Lett. 2014;104:261112. https://doi.org/10.1063/1.4886761.
22. Abellán C, Amaya W, Jofre M, Curty M, Acín A, Capmany J, Pruneri V, Mitchell MW. Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode. Opt Express. 2014;22:1645–54. https://doi.org/10.1364/OE.22.001645.
23. Jofre M, Curty M, Steinlechner F, Anzolin G, Torres J, Mitchell M, Pruneri V. True random numbers from amplified quantum vacuum. Opt Express. 2011;19:20665–72. https://doi.org/10.1364/OE.19.020665.
24. Qi B, Chi Y-M, Lo H-K, Qian L. High-speed quantum random number generation by measuring phase noise of a single-mode laser. Opt Lett. 2010;35:312–4. https://doi.org/10.1364/OL.35.000312.
25. Mitchell M, Abellan C, Amaya W. Strong experimental guarantees in ultrafast quantum random number generation. Phys Rev A. 2015;91:012314. https://doi.org/10.1103/PhysRevA.91.012314.
26. Xu F, Qi B, Ma X, Xu H, Zheng H, Lo H-K. Ultrafast quantum random number generation based on quantum phase fluctuations. Opt Express. 2012;20:12366–77. https://doi.org/10.1364/OE.20.012366.
27. Henry C. Theory of the linewidth of semiconductor lasers. IEEE J Quantum Electron. 1982;18:259–64. https://doi.org/10.1109/JQE.1982.1071522.
28. Rudé M, Abellan C, Capdevila A, Doménech J, Mitchell M, Amaya W, Pruneri V. Interferometric photodetection in silicon photonics for phase diffusion quantum entropy sources. Opt Express. 2018;26:31957. https://doi.org/10.1364/OE.26.031957.
29. Imran M, Sorianello V, Fresi F, Jalil B, Romagnoli M, Potì L. On-chip tunable SOI interferometer for quantum random number generation based on phase diffusion in lasers. Opt Commun. 2021;485:126736. https://doi.org/10.1016/j.optcom.2020.126736.
30. Abbasi A, Verbist J, Van Kerrebrouck J, Lelarge F, Duan G-H, Yin X, Bauwelinck J, Roelkens G, Morthier G. 28 Gb/s direct modulation heterogeneously integrated C-band InP/SOI DFB laser. Opt Express. 2015;23:26479–85. https://doi.org/10.1364/OE.23.026479.
31. Abellan C, Amaya W, Doménech J, Muñoz P, Capmany J, Longhi S, Mitchell M, Pruneri V. Quantum entropy source on an InP photonic integrated circuit for random number generation. Optica. 2016;3:989–94. https://doi.org/10.1364/OPTICA.3.000989.
32. Roger T, Paraiso T, De Marco I, Marangon DG, Yuan Z, Shields AJ. Real-time interferometric quantum random number generation on chip. J Opt Soc Am B. 2019;36:B137–42. https://doi.org/10.1364/JOSAB.36.00B137.
33. Septriani B, De Vries O, Steinlechner F, Gräfe M. Parametric study of the phase diffusion process in a gain-switched semiconductor laser for randomness assessment in quantum random number generator. AIP Adv. 2020;10:055022. https://doi.org/10.1063/5.0011418.
34. Lovic V, Marangon DG, Lucamarini M, Yuan Z, Shields AJ. Characterizing phase noise in a gain-switched laser diode for quantum random-number generation. Phys Rev Appl. 2021;16:1. https://doi.org/10.1103/PhysRevApplied.16.054012.
35. Shakhovoy R, Tumachek A, Andronova N, Mironov Y. Phase randomness in a gain-switched semiconductor laser: stochastic differential equation analysis. p. 14–17.
36. Martin A, Sanguinetti B, Lim CCW, Houlmann R, Zbinden H. Quantum random number generation for 1.25-GHz quantum key distribution systems. J Lightwave Technol. 2015;33:2855–9.
37. Yang J, Fan F, Liu J, Su Q, Li Y, Huang W, Xu B. Randomness quantification for quantum random number generation based on detection of amplified spontaneous emission noise. Quantum Sci Technol. 2020;6:15002. https://doi.org/10.1088/2058-9565/abbd80.
38. Guo Y, Cai Q, Li P, Jia Z, Xu B, Zhang Q, Zhang Y, Zhang R, Gao Z, Shore KA, Wang Y. 40 Gb/s quantum random number generation based on optically sampled amplified spontaneous emission. APL Photon. 2021;6:66105. https://doi.org/10.1063/5.0040250.
39. Bassham L, Rukhin A, Soto J, Nechvatal J, Smid M, Leigh S, Levenson M, Vangel M, Heckert N, Banks D. A statistical test suite for random and pseudorandom number generators for cryptographic applications. 2010. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=906762.