Research Article | Vol. 26, No. 16 | 6 Aug 2018 | OPTICS EXPRESS 19730
Optics EXPRESS

Generation of random numbers by measuring phase fluctuations from a laser diode with a silicon-on-insulator chip

FRANCESCO RAFFAELLI,[1,*] PHILIP SIBSON,[1] JAKE E. KENNARD,[1] DYLAN H. MAHLER,[1,2] MARK G. THOMPSON,[1] AND JONATHAN C. F. MATTHEWS[1]

[1]*Quantum Engineering Technology Labs, Department of Physics, Tyndall Avenue, University of Bristol, Bristol BS8 1TH, UK*
[2]*Now at: Xanadu, 372 Richmond St W, Toronto, ON M5V 2L7, Canada*
[*]*francesco.raffaelli@bristol.ac.uk*

Abstract: Random numbers are a fundamental resource in science and technology. Among the different approaches to generating them, random numbers created by exploiting the laws of quantum mechanics have proven to be reliable and can be produced at enough rates for their practical use. While these demonstrations have shown very good performance, most of the implementations using free-space and fibre optics suffer from limitations due to their size, which strongly limits their practical use. Here we report a quantum random number generator based on phase fluctuations from a diode laser, where the other required optical components are integrated on a mm-scale monolithic silicon-on-insulator chip. The post-processing reported in this experiment is performed via software. However, our physical device shows the potential of operation at generation rates in the Gbps regime. Considering the device's size, its simple, robust and low power operation, and the rapid industrial uptake of silicon photonics, we foresee the widespread integration of the reported design in more complex systems.

OCIS codes: (130.3120) Integrated optics devices; (270.5565) Quantum communications; (270.5585) Quantum information and processing.

References and links

1. M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum random number generators," Rev. Mod. Phys. **89**, 015004 (2017).
2. J. Rarity, P. Owens, and P. Tapster, "Quantum random-number generation and key sharing," J. Mod. Opt. **41**(12), 2435–2444 (1994).
3. T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, "A fast and compact quantum random number generator," Rev. Sci. Instrum. **71**(4), 1675–1680 (2000).
4. C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauerer, U. L. Andersen, C. Marquardt, and G. Leuchs, "A generator for unique quantum random numbers based on vacuum states," Nat. Photon. **4**, 711–715 (2010).
5. Y. Shen, L. Tian, and H. Zou, "Practical quantum random number generator based on measuring the shot noise of vacuum states," Phys. Rev. A **81**, 063814 (2010).
6. T. Symul, S. M. Assad, and P. K. Lam, "Real time demonstration of high bitrate quantum random number generation with coherent laser light," Appl. Phys. Lett. **98**(23) (2011).
7. M. Avesani, D. G. Marangon, G. Vallone, and P. Villoresi, "High speed continuous variable source-independent quantum random number generation," arXiv preprint arXiv:1709.00685v1 [quant-ph] (2017).
8. B. Xu, Z. Li, J. Yang, S. Wei, Q. Su, W. Huang, Y. Zhang, and H. Guo, "High speed continuous variable source-independent quantum random number generation," arXiv preprint arXiv:1709.00685v1 [quant-ph] (2017).
9. 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**, 312–314 (2010).
10. F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng, and H.-K. Lo, "Ultrafast quantum random number generation based on quantum phase fluctuations," Opt. Express **20**, 12366–12377 (2012).
11. Y.-Q. Nie, L. Huang, Y. Liu, F. Payne, J. Zhang, and J.-W. Pan, "The generation of 68 gbps quantum random number by measuring laser phase fluctuations," Rev. Sci. Instrum. **86**(6) (2015).

#328578 https://doi.org/10.1364/OE.26.019730
Journal © 2018 Received 17 Apr 2018; revised 8 Jun 2018; accepted 11 Jun 2018; published 23 Jul 2018

Optics EXPRESS

12. 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**, 20665–20672 (2011).
13. 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**, 1645–1654 (2014).
14. R. Sakuraba, K. Iwakawa, K. Kanno, and A. Uchida, "Tb/s physical random bit generation with bandwidth-enhanced chaos in three-cascaded semiconductor lasers," Opt. Express **23**, 1470–1490 (2015).
15. B. Sanguinetti, A. Martin, H. Zbinden, and N. Gisin, "Quantum random number generation on a mobile phone," Phys. Rev. X **4**, 031056 (2014).
16. C. Abellan, W. Amaya, D. Domenech, P. M. noz, J. Capmany, S. Longhi, M. W. Mitchell, and V. Pruneri, "Quantum entropy source on an inp photonic integrated circuit for random number generation," Optica **3**, 989–994 (2016).
17. F. Raffaelli, G. Ferranti, D. H. Mahler, P. Sibson, J. E. Kennard, A. Santamato, G. Sinclair, D. Bonneau, M. G. Thompson, and J. C. F. Matthews, "A homodyne detector integrated onto a photonic chip for measuring quantum states and generating random numbers," Quantum Sci. Technol. **3**(2), 025003 (2018).
18. P. Sibson, C. Erven, M. Godfrey, S. Miki, T. Yamashita, M. Fujiwara, M. Sasaki, H. Terai, M. G. Tanner, C. M. Natarajan, R. H. Hadfield, J. L. O'Brien, and M. G. Thompson, "Chip-based quantum key distribution," Nat. Commun. **8**, 13984 (2017).
19. P. Sibson, J. E. Kennard, S. Stanisic, C. Erven, J. L. O'Brien, and M. G. Thompson, "Integrated silicon photonics for high-speed quantum key distribution," Optica **4**, 172–177 (2017).
20. Y. Ding, D. Bacco, K. Dalgaard, X. Cai, X. Zhou, K. Rottwitt, and L. K. Oxenlowe, "High-dimensional quantum key distribution based on multicore fiber using silicon photonic integrated circuits," npj QI **3** (2017).
21. C. Ma, W. D. Sacher, Z. Tang, J. C. Mikkelsen, Y. Yang, F. Xu, T. Thiessen, H.-K. Lo, and J. K. S. Poon, "Silicon photonic transmitter for polarization-encoded quantum key distribution," Optica **3**, 1274–1278 (2016).
22. B. Haylock, D. Peace, F. Lenzini, C. Weedbrook, and M. Lobino, "Multiplexed quantum random number generation," arXiv preprint arXiv:1801.06926 [quant-ph] (2018).
23. S.-H. Sun and F. Xu, "Experimental study of a quantum random-number generator based on two independent lasers," Phys. Rev. A **96**, 062314, Dec 2017.
24. K. Petermann, "Laser Diode Modulation and Noise," (Kluwer Academic Publishers) (1988).
25. C. Henry, "Theory of the linewidth of semiconductor lasers," IEEE J. Quant. Electron. QE-**18**(2), 259–264 (1982).
26. K. Vahala and A. Yariv, "Occupation fluctuation noise: A fundamental source of linewidth broadening in semiconductor lasers," Appl. Phys. Lett. **43**(2), 140–142 (1983).
27. P. P. Absil, P. De Heyn, H. Chen, P. Verheyen, G. Lepage, M. Pantouvaki, J. De Coster, A. Khanna, Y. Drissi, D. Van Thourhout, and J. Van Campenhout, "Imec isipp25g silicon photonics: a robust cmos-based photonics technology platform," Proc. SPIE **9367** (2015).
28. X. Ma, F. Xu, H. Xu, X. Tan, B. Qi, and H.-K. Lo, "Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction," Phys. Rev. A **87**, 062327 (2013).
29. M. W. Mitchell, C. Abellan, and W. Amaya, "Strong experimental guarantees in ultrafast quantum random number generation," Phys. Rev. A **91**, 012314 (2015).
30. http://csrc.nist.gov/groups/ST/toolkit/rng/.
31. K. Kaur, A. Subramanian, P. Cardile, R. Verplancke, J. V. Kerrebrouck, S. Spiga, R. Meyer, J. Bauwelinck, R. Baets, and G. V. Steenberge, "Flip-chip assembly of vcsels to silicon grating couplers via laser fabricated su8 prisms," Opt. Express **23**, 28262–28270 (2015).
32. J. Wang, S. Paesani, Y. Ding, R. Santagati, P. Skrzypczyk, A. Salavrakos, J. Tura, R. Augusiak, L. Mančinska, D. Bacco, D. Bonneau, J. W. Silverstone, Q. Gong, A. Acín, K. Rottwitt, L. K. Oxenløwe, J. L. O'Brien, A. Laing, and M. G. Thompson, "Multidimensional quantum entanglement with large-scale integrated optics," Science, 10.1126/science.aar7053 (2018).
33. M. Rude, C. Abellan, A. Capdevila, D. Domenech, M. W. Mitchell, W. Amaya, V. Pruneri, "Phase diffusion quantum entropy source on a silicon chip," arXiv preprint arXiv:1804.04482 [quant-ph] (2018).
34. F. Raffaelli, P. Sibson, J. E. Kennard, D. H. Mahler, M. G. Thompson, J. C. F. Matthews, "Generation of random numbers by measuring phase fluctuations from a laser diode with a silicon-on-insulator chip," https://data.bris.ac.uk/data/dataset/10.5523/bris.2nvzdjr7gy4ox2njh7a6tbwks6

1. Introduction

In the last few decades [1], quantum random number generators (QRNG) have been demonstrated with different optical systems such as single photons [2, 3], optical vacuum states [4, 6–8], phase fluctuations from a laser diode [9–13] and chaotic lasers [14]. Among all these schemes, the QRNGs based on phase fluctuations from a laser diode achieved the highest generation rates, up 68 Gbps [11]. On one hand, this fast development shows the relevance of QRNG to modern science and technology. On the other hand, it must be noticed how all the aforementioned works were performed either with bulk or fibre components, leading to strong practical limitations. First, given the size of the components used, these devices are difficult to integrate into more complex

Optics EXPRESS

systems, such as a Quantum Key Distribution (QKD) receiver or a CPU. Second, the cost of each component is considerable, severely reducing scalability. Finally, bulk fibre optics devices often suffer from instability issues, limiting their use in real-world scenarios.

In order to build more practical devices, the community started looking into ways to reduce the size of QRNGs. Sanguinetti et al. [15] demonstrated a QRNG taking advantage of a smartphone camera. Abellan and co-workers [16] demonstrated a random number generator fully integrated into a Indium Phosphide (InP) microchip and Raffaelli et al. [17] demonstrated a Silicon-on-Insulator (SOI) QRNG, using the scheme proposed by Gabriel and colleagues [4]. Interestingly [16] and [17] were performed in the same platforms used for the first prototypes of integrated QKD devices [18–21], supporting potential integration in the future. Recently, Haylock et. al [22] demonstrated multiplexing of the scheme reported in [4], in the Lithium Niobate (LN) platform — this multiplexed approach allows enhanced generation rates, but the relatively large footprint of LN can limit the possibility of integrating LN chips into more complex systems. In this sense, the InP based QRNG [16] provides a more attractive solution, but it has the extra requirement of RF modulation to control the laser, which in turn limits the generation rate [23]. The experiment by Raffaelli et al., based on homodyne measurements, does not present this complication. However, it does require optical powers one order of magnitude higher than those used in laser diode phase fluctuations implementations [10, 11]. This can be problematic since high optical powers in integrated photonics introduces negative side effects such as temperature variations and optical cross talk, potentially detrimental if integrated in systems with a high density of components. Here, in order to overcome these limitations, we combined the advantages of [10, 11] with the ultra-small footprint and versatility of the silicon-on-insulator platform, reporting the demonstration of a SOI integrated QRNG based on phase fluctuations from a diode laser.

2. Results

The technique used here lies on the intrinsic properties of laser emission. For any laser, the emitted light is given by a contribution from the stimulated emission and a contribution from the spontaneous emission [24–26]. The spontaneous emission, characterised by random phase fluctuations, can be efficiently exploited to generate true random numbers [10, 11]. In [10, 11] the theory behind this scheme can be found and briefly reported below. The electromagnetic field of the emitted light from a laser diode can be expressed as

$$E(t) = Ee^{-i(\omega t+\theta(t))}, \tag{1}$$

where ω is the angular frequency of the electromagnetic field and $\theta(t)$ is a random phase due to the contribution of the spontaneous emission to the emitted light. In order to take advantage of the random phase-fluctuations of the electromagnetic field, the light is injected into an unbalanced Mach-Zehnder interferometer (MZI). After removing the DC components, the intensity at the photodiodes will be given by

$$I(t) \propto P\sin(\Delta\theta(t)) \sim P\Delta\theta(t), \tag{2}$$

where the first equation holds when the phase delay due to the different length between the two arms of the MZI is $2m\pi + pi/2$, and the second relation is valid for small values of $\Delta\theta(t)$. The light intensity at the photodiodes is converted into voltage signal by a transimpedance amplifier and the variance of the voltage measured by the oscilloscope is

$$\sigma^2 \equiv \langle\Delta V(t)^2\rangle \propto AP^2\langle\Delta\theta(t)^2\rangle + F, \tag{3}$$

where $\sigma^2 \equiv \langle\Delta\theta(t)^2\rangle$ is the variance of the phase noise, A is a conversion constant between the optical power and voltage variance, which takes into account the responsivity of the photodiodes

Optics EXPRESS

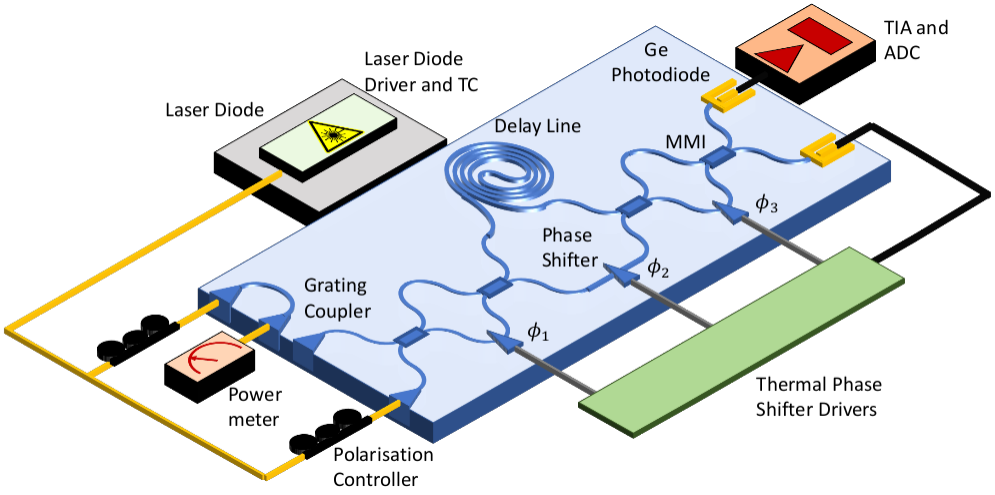

Fig. 1. Setup of the experiment. a) A diode laser, controlled by a laser diode driver and temperature stabilised by a temperature controller, is used to operate just above threshold. A minimal part of the light is sent to a polarisation controller and coupled into a test waveguide, to monitor the coupling losses. The rest of light is sent to a polarisation controller and then coupled into the cascade of Mach-Zehnder interferometers. While the first and last MZIs serve as tunable beam-splitter, the central, unbalanced MZI converts the phase-fluctuations into intensity fluctuations. Two photodiodes are place at the output of the cascade. One of them is used as a monitor, and it allows to calibrate the phase of the interferometers. This is achieved through heater drivers, which control the phase of the MZIs by applying voltage to the integrated phase-shifters. The second photodiode is connected to a transimpedance amplifier, converting the light intensity fluctuations into voltage fluctuations. These fluctuations are digitalised by a oscilloscope to generate random bits.

and gain of the amplifying electronics, and F is the variance of the background electronic noise. It can be shown [25, 26] that the variance of the random phase of a diode laser is the sum of an intrinsic quantum phase noise Q and a classical phase noise C and it can be expressed as

$$\langle \Delta\theta(t)^2 \rangle = (\frac{Q}{P} + C). \tag{4}$$

As a consequence, the variance of the voltage becomes

$$\sigma^2 = ACP^2 + AQP + F, \tag{5}$$

and the parameters AC, AQ and F, dependent on the specific laser and measurement setup, can be determined through a polynomial fit. As mentioned above, the phase noise intrinsic to the spontaneous emission is expressed by the parameter AQ in Eq. (5). Therefore, we define the Quantum-to-Classical Noise Ratio (QCNR) as

$$QCNR = \frac{AQP}{ACP^2 + F}. \tag{6}$$

2.1. Description of the experimental setup

In Fig. 1 we report a scheme of our experiment. A Mitsubishi FU-68SDF-8 DFB laser diode, driven by a Thorlabs CLD1015 module, was used as a light source. The light was sent to a polarisation controller to optimise the coupling of the optical beam on chip. The vertical

Optics EXPRESS

coupling was achieved by using a 8-channel V-groove array (VGA), coupled into the single mode waveguides with grating couplers. Part of the light, during the characterisation process, was sent through a test waveguide to a power meter for monitoring the coupling losses into the chip. The SOI chip used for this experiment was designed using iSiPP25G technology and manifactured by IMEC [27]. Our QRNG was characterised by a cascade of three Mach-Zehnder interferometers. Indeed, Eq. (2) is based on the assumption of perfectly balanced beam-splitter and lossless optical channel. When working in bulk and fibre optics these assumptions are satisfied to a very high degree. However, fabrication errors in integrated SOI devices can drastically alter the reflectivity. For example, the integrated multi-mode interferometers (MMIs) used in our experiment have show around 0.5 dB excess loss. Moreover, the linear losses in our single mode waveguides are estimated to be 2-3 dB/cm, not negligible in a long delay line. This implies that the physical device must be designed in such a way to take into account the imperfections in the integrated device. Therefore, the input and output MZIs, controlled by ϕ_1 and ϕ_3, were balanced MZIs, where the length of the two arms was equal, and the relative phase between the two arms could be tuned by taking advantage of a thermal phase-shifter. These MZIs formed tunable reflectivity beam-splitters. The central MZI, controlled by ϕ_2, was instead unbalanced, with a time delay $T_d \sim 540$ ps (corresponding to ~ 4 cm length) between the two arms, which allowed mapping the fluctuations in the phase of the electromagnetic field into intensity fluctuations. This central MZI presented a phase-shifter used to configure the system to optimise the intensity fluctuations. Indeed, Eq. (2) is based on the assumption of perfectly balanced beam-splitter and lossless optical channel. When working in bulk and fibre optics these assumptions are satisfied to a very high degree. However, fabrication errors in integrated SOI devices can drastically alter the reflectivity. For example, the integrated multi-mode interferometers (MMIs) used in our experiment have show around 0.5 dB excess loss. Moreover, the linear losses in our single mode waveguides are estimated to be 2-3 dB/cm, not negligible in a long delay line. This implies that the physical device must be designed in such a way to take into account the imperfections in the integrated device. Therefore, the input and output MZIs, controlled by ϕ_1 and ϕ_3, were balanced MZIs, where the length of the two arms was equal, and the relative phase between the two arms could be tuned by taking advantage of a thermal phase-shifter. These MZIs formed tunable reflectivity beam-splitters. The central MZI, controlled by ϕ_2, was instead unbalanced, with a time delay $T_d \sim 540$ ps (corresponding to ~ 4 cm length) between the two arms, which allowed mapping the fluctuations in the phase of the electromagnetic field into intensity fluctuations. This central MZI presented a phase-shifter used to configure the system to optimise the intensity fluctuations. The choice of the delay is related to the coherence time of the laser ($\tau_{coh} \sim 2.5$ ns) and the achievable sampling rate of the ADC. Indeed, the coherence time of the laser must be greater than the delay time for Eq. (2) to hold. On the other hand, the variance of the phase noise goes as $\langle \Delta\theta(t)^2 \rangle = 2T_d/\tau_{coh}$ ([9]) and therefore, for a given τ_{coh}, a very short delay line would reduce the variance of the phase fluctuations. At the same time the condition $1/T_d > \mathrm{S}$ (where S is the sampling rate) must hold. Hence, a very short delay line would also require designing a faster TIA. However, designing low noise, high speed TIAs is challenging and given the low optical powers involved in our experiment, a delay line of 540 ps satisfies both the constraints imposed by the coherence time of the laser and the electronics bandwidth.

While most of the waveguides were standard strip single mode waveguides with a 220 nm $\times$ 450 nm cross section, the delay line was characterised by a broader rib waveguide to limit the losses. The MZIs cascade was designed with two Ge photodiodes at the outputs (23 GHz bandwidth, nominal value given by the foundry). The first photodiode was used to monitor the optical power, and it could be used to vary the phase of the integrated phase-shifters, through heater drivers controlled via computer. The photo-current from the second photodiode was converted into a voltage signal and amplified by a custom made high-speed, low-noise transimpedance amplifier (TIA). The voltage signal was detected and digitalised by a fast GHz

Optics EXPRESS

bandwidth oscilloscope (DSOV134A Agilent Keysight Technology) and the data were further analysed and post-processed by a desktop computer, to extract random bits. In practise, the grating couplers, MZI and photodiodes occupied an area $< 1\text{mm}^2$, integrated on a SOI chip with a footprint of 2.5 mm × 2.5 mm. The chip was embedded and wirebonded to a 4 cm × 8 cm electronic printed circuit board, containing the TIA and the voltage supply for the photodiodes. This system was enclosed inside a Faraday cage, to reduce the RF environmental noise.

2.2. Determination of the quantum-to-classical noise ratio QCNR

To estimate the QCNR, for each value of the input current, the maximum phase noise variance had been extracted after scanning the phase ϕ_2 over 2π. Then, the variance was plotted as a function of the optical power, shown in Fig. 2(a). After this, the parameters AC, AQ and F were determined by using a quadratic least square algorithm, and consequently it was possible to extract the QCNR, reported in Fig. 2(b) (blue continuous line). The parameter of the fit are

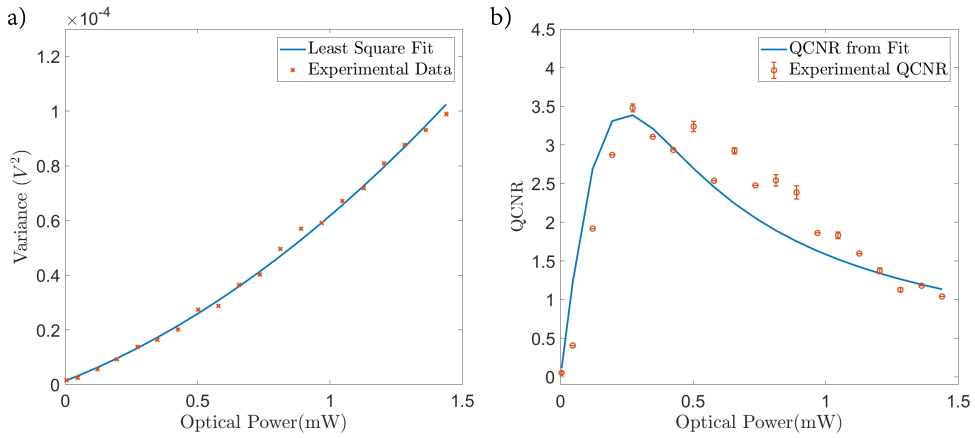

Fig. 2. Phase-fluctuations variance and QCNR as a function of the optical power. a) Quadratic fit of the noise variance. b) In blue the QCNR extracted by the quadratic fit. In orange, the experimentally determined QCNR.

reported in Table 1.

Table 1. **The statistical parameters for the fit of the voltage noise variance as a function of the optical power.**

Parameter	Value
AC(V/W^2)	22.519
AQ(V/W)	0.03784
F (V)	1.3732×10^{-6}
R-Squared	0.998

A second experimental approach, suggested in [10], was used to verify the QCNR. This second approach has the main advantage that the QCNR can be estimated experimentally for a single given value of the power. It relies on the fact that the phase-fluctuations are due to a quantum contribution, that we called Q and a classical contribution that we called C. The quantum contribution will be dominant when the laser is operated just above threshold, while the classical contribution will be dominant when the laser diode is operated with a high input currents. Hence, in order to estimate the QCNR experimentally, first of all we measured the

Optics EXPRESS

variance σ^2 for a given power P_0. This was then compared to the variance σ^2_{att} measured when the laser was operated in the classical regime (at maximum power) and attenuated with a variable optical attenuator (VOA) to obtain the same optical power P_0.

Finally, we calculated the ratio $QCNR_{exp} = \frac{\sigma^2 - \sigma^2_{att}}{\sigma^2_{att}}$ which gave the ratio between the pure quantum contribution and the contribution due to the classical noise. The experimentally measured QCNR is shown in Fig. 2(b) (red circles). Here we observe a good agreement between the QCNR obtained with the two methods. The discrepancy for some points with the fit is due to the fact that, given the high input losses of the VOA, we had to manually remove the VOA to obtain σ^2. This operation slightly affected the polarisation and thus the coupled optical power into the chip. Here it is worth noting that the optical power, reported in the x-axis in Fig. 2, is the optical power before coupling into the chip. This is one order of magnitude lower than the optical power used in [17]. This demonstration at lower optical powers allows mitigation against potentially negative effects such as self phase modulation and optical cross talk, making this scheme more suitable for integration in more complex systems.

2.3. Estimation of the min-entropy H_∞

Similarly to [28], in the order to estimate the maximum extractable randomness, the min-entropy of the digitalised voltage signal can be calculated.

$$\mathrm{H}_\infty = -\log_2\left(\max_{x\in\{0,1\}^n} \Pr[X = x]\right) \tag{7}$$

is the min-entropy, where n is the number of bits used in the digitalisation of the voltage signal and $\Pr[X = x]$ is the probability of the voltage measurement x, falling in the X bin. The min-entropy is related with the maximum guessing probability under the assumption that the distribution is known. Hence, Eq. (7) holds only for uncorrelated bits and for a quantum signal independent from the classical signal. In Fig. 3 it can be seen that the optical signal is characterised by a nearly flat spectrum within the bandwidth and well above the electronics noise background, which was affected by environmental noise and thus would inevitably present correlations. This confirms the assumption of a quantum signal independent from the classical noise. Moreover, the hypothesis of uncorrelated bits is confirmed by the low values of the correlations in Fig. 4(a) for the 500 Msamples/s line. Finally, in order to extract information about the quantum state, we must be able to recover information about the ratio between the quantum and classical noise, given that the measured sample is a contribution of both quantum and classical part. It can be shown that $\Delta V(t)$ has a gaussian distribution, being the linear combination of three different gaussian contributions. For this reason, the voltage variance due to the quantum phase-fluctuations can be obtained as

$$\sigma^2_q = \frac{\sigma^2}{1 + \frac{1}{QCNR}}. \tag{8}$$

For a discrete probability distribution as the one measured by the oscilloscope, the estimated min-entropy for the quantum signal was ultimately determined by the QCNR, the number of bits and voltage range of the oscilloscope. In particular, the voltage range cannot be neither too small because would lead to loss of part of the signal, nor too big because otherwise the samples will be concentrated in the central bins which would reduce the unpredictability of the outcomes. Moreover, in our proof principle we assumed that the digitization process is independent from the quantum signal and therefore it does not affect the min-entropy. Further analysis on digitization errors was explained in [29], where more conservative assumptions are made on the classical hardware involved in the measurements. This approach will be taken into account for future real-time demonstrations of our integrated QRNGs.

The following procedure was used to determine the min-entropy. For different values of the optical power, we swept the phase of the central interferometer from 0 to π, recording the fringes

Optics EXPRESS

of the variance. Then, for each optical power, we selected the maximum variance from the fringe and we plotted the maximum variance as a function of the optical power. The next step consisted in extracting the QCNR by using Eq. (6). Once we had determined the QCNR, we calculated σ_q^2, by making use of Eq. (8). We then chose a voltage range in the oscilloscope to optimise the information contained in the measured signal (in our case $V(max, min) = \pm 5\sigma$) and divided the interval into 2^8 bins, due to the resolution of our oscilloscope. Finally, we integrated the signal over the bins and normalized the distribution to obtain $Pr[x]$ as in Eq. (7) and calculated the min-entropy H_∞. As shown in the previous paragraphs, we obtained QCNR $\sim$ 3.38. As a combination of these factors, we estimated the min-entropy to be $H_\infty \sim 5.6$ bits/sample. This value of the entropy was used to implement a software version of the Toeplitz extractor [28], that allowed us to obtain uniformly distributed random bits.

2.4. Bandwidth and generation rate estimation

In order to determine the optimal sampling rate of the device, the spectral density of our QRNG was measured in absence and presence of the optical signal. The result is reported in Fig. 3. The detector has appreciable dark noise clearance up to a speed of approximately 500 MHz. This is a direct consequence of the specific operational amplifier used and layout of the electronics. The gain of the TIA was chosen to be 5kΩ. The reason for this choice was due to the operational amplifier selected, a LT6268-10 from Linear Technology. This operational amplifier is stable for values similar or above 5kΩ. Here we notice that the photodiodes are more than one order of magnitude faster than the TIA. Therefore, the spectral properties of the analog voltage signal are almost completely determined by the speed of the TIA. The sampling rate is chosen in order not to oversample the analog signal, in agreement with the analysis developed in [5]. From Fig. 3 we can also see some peaks, mainly around 100 MHz, which are the radio environmental noise. However, the signal is well above the noise floor, so the environmental noise does not influence the generation of random bits. Taking into account a sampling rate of 500 Msamples, and that $H_\infty = 5.6$ bits/sample, when sampling at 8 bits/sample, we estimated a potential randomness generation rate of nearly 2.8 Gbps. We note that the generation rate is more than one order of magnitude lower than in [11]. This is mainly due to the limited bandwidth of our low-noise TIA. A faster TIA combined with lower loss grating couplers and optimization in the waveguides design would allow to increase the generation rate beyond 10 Gbps.

2.5. Autocorrelations and statistical tests

A first estimation of the quality of the bit sequences is given by the autocorrelations of the samples. In fact, environmental RF noise, oscillations of the transimpedance amplifier and oversampling are the main cause of periodic oscillations in the signal that can result in correlated bit sequences. Moreover, since these factors can be in principle controlled classically by an adversary, it is important to study the autocorrelation of the signal to make sure about the unpredictability of the random bits. For this reason we measured the autocorrelation of the signal, acquired at different sampling rates. As expected, the optimal sampling rate appears to be 500 Msamples/s. This is because of the spectral density of the detector, where the optical signal is well above the electronic noise up to 500 MHz. On the other hand, oversampling at 5 Gsamples/s results in highly correlated sequences, as shown by the yellow line in Fig. 4(a).

A second characterization of the randomness was achieved by taking advantage of the statistical tests provided by the National Institute of Standards and Technology (NIST SP 800-22). As can be seen in Table 2 and Fig. 5, the hashed bits passed all the statistical tests.

2.6. Stability

Among the main advantages of working with integrated photonics there are the potentially ultra-small footprint and monolithic nature of the devices. While compactness allows for parallelization

Optics EXPRESS

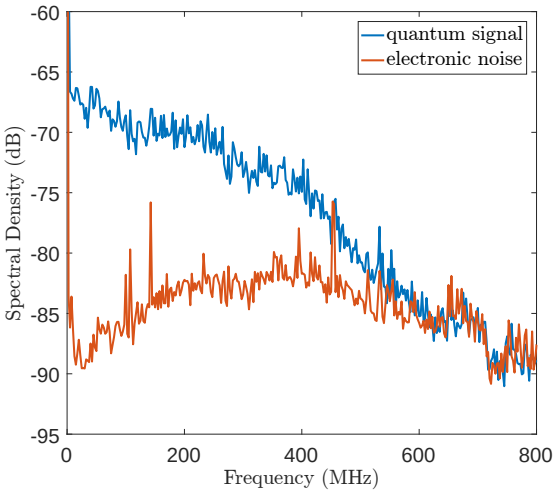

Fig. 3. Spectral density for quantum signal and noise floor. Here the spectral density for the optical signal and for the electronic noise floor are reported. It can be observed that the quantum signal is above the electronic noise up to 500 MHz. The noise floor presents some peaks due to environmental noise, particularly around 100 MHz. These are the FM radio signal, which however are below the quantum signal and therefore are not affecting the quality of the generated random numbers.

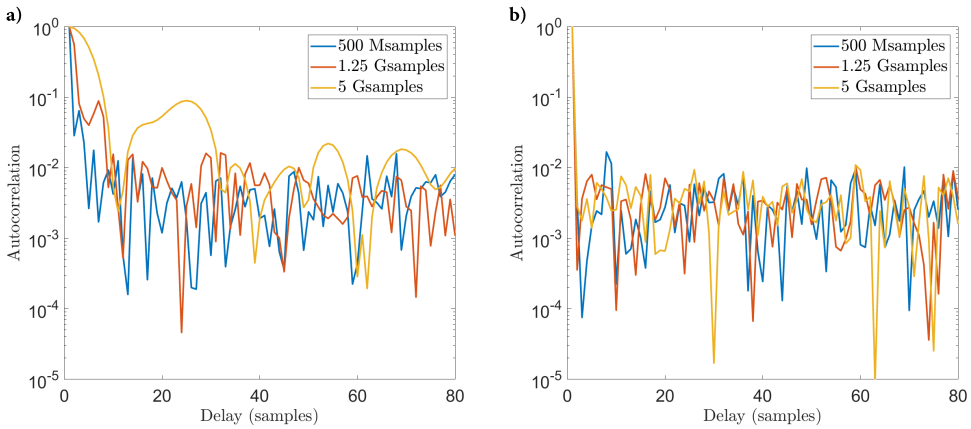

Fig. 4. Autocorrelation of raw and hashed bits. a) Here we report the autocorrelations of the raw signal, obtained after digitizing the signal, for different sampling rates. We notice that for sampling speeds above the bandwidth the autocorrelations can be up to one order of magnitude bigger than the when sampling at 500 Msamples. b) The hashing reduces drastically the autocorrelations. No appreciable difference can be observed in this case between different sampling speeds.

of multiple components into a single microchip, the monolithic nature has the main advantage of strongly reducing many forms of instability. This is particularly useful when dealing with interferometry and unbalanced interferometers. For example, when working with optical fibres, small changes in temperature can affect the length of the fibre enough to destroy interference. In bulk optics instead, the stability is threatened by any environmental factor that generates

Optics EXPRESS

Table 2. **Here we report the results for the NIST (National Institute of Standards & Technology) statistical tests suite [30]. In order to pass the NIST SP800-22 the pass rate must be above 0.98 for each type of test (column II) and the reported P-values, which refer to the uniformity test on the distributions plotted in Fig. 5, must be above 0.01 (column III).**

NIST SP800-22		
Test name	Pass Rate	P-value
Frequency	0.989	0.891
Block Frequency	0.993	0.128
Cumulative Sums	0.987	0.186
Runs	0.989	0.177
Longest Run	0.992	0.768
Rank	0.995	0.360
FFT	0.984	0.465
Non Overlapping Template	0.995	0.014
Overlapping Template	0.986	0.155
Universal	0.985	0.800
Approximate Entropy	0.984	0.573
Random Excursions	0.993	0.115
Random Excursions Variant	0.989	0.011
Serial	0.991	0.169
Linear Complexity	0.993	0.768

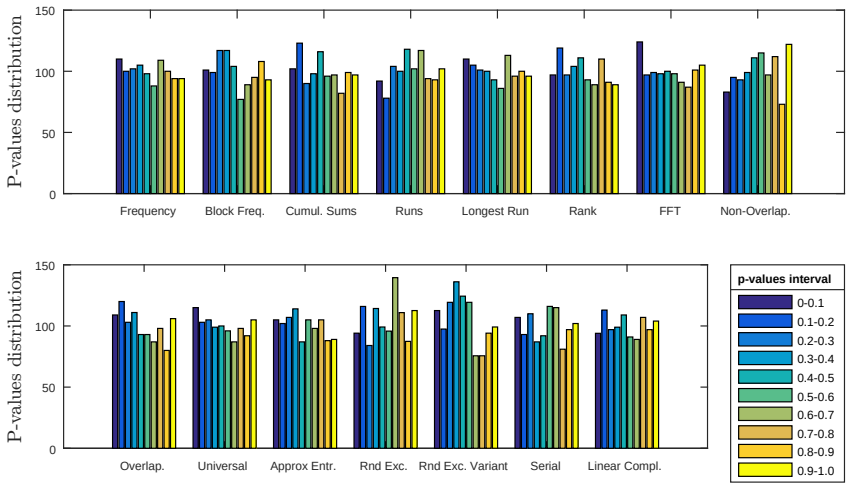

Fig. 5. Uniformity test for the P-values. Under the assumption that the produced random bits are truly random, the P-values must be uniformly distributed between 0 and 1. Here the NIST statistical test provides the frequencies of the P-values, by dividing the (0,1) interval into 10 sub-intervals. We can observe that for each test the P-values are uniformly distributed.

oscillations in the optics. By reducing the size of the systems, and by integrating everything in a single chip, these issues are drastically reduced. This fact was particularly relevant in our experiment. In fact, as can be observed in the red line of Fig. 6, the system was highly stable

Optics EXPRESS

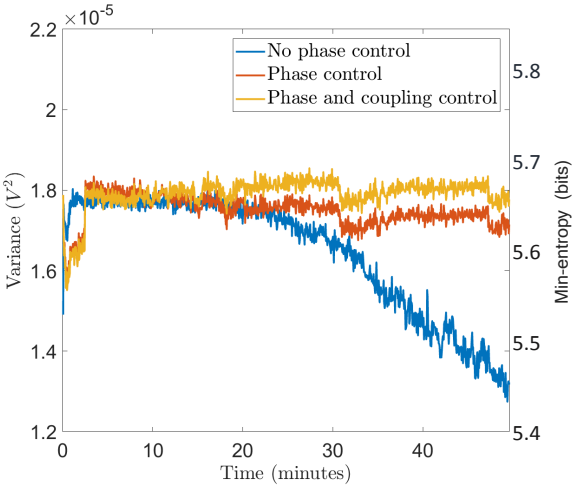

Fig. 6. Signal variance measured over a time interval of one hour. In this picture the variance of the signal measured by the oscilloscope was measured over a time interval of 50 minutes. The blue line shows the behaviour of the variance without any control on the phase of the integrated MZIs. The red line shows the variance when the phase of the unbalanced MZI have been calibrated every 2 minutes. The yellow line has been obtained by normalising the variance plotted in red with the optical power coupled into the chip. It can be seen than, beside some variation due to the change in the fibre-chip coupling, a phase calibration every few minutes is sufficient to keep the system perfectly balanced.

in a time range of almost one hour. This was obtained by simply calibrating the phase of the unbalanced interferometer every 2-3 minutes (red line). Moreover, even without any calibration in the phase of the interferometer, the variance of the signal (blue line), was stable over a time interval of several minutes. Here it is important to remark that only the voltage in the unbalanced interferometer was scanned, while phase-shifters 1 and 3 remained untouched after a initial characterisation. Furthermore, the yellow line was obtained normalising the variance taking into account the small variation in the optical power, due mainly to changes in polarisation in the light off-chip. In both the yellow and red lines, some steps in the variance can be observed. These steps are due to the fact that, while recalibrating the phase ϕ_2, the point of maximum variance had slightly shifted. In Fig. 6, on the right vertical axis, we plotted the min-entropy obtained for that particular voltage variance. From this, it can be see that the system is very stable, allowing the entropy to be kept unchanged within the unity over a time interval of one hour, even without applying any phase control.

3. Discussion

In conclusion, we report the demonstration of a SOI integrated version of a QRNG based on phase fluctuations from a laser diode, where all the optical components and photodiodes are integrated onto a single monolithic microchip and fibre coupled to a laser diode. We showed that high rates of random numbers can be achieved with sub mW optical powers, one order of magnitude lower the previous QRNG demonstrated in a SOI device [17]. Compared to [10, 11], our ultra-compact QRNG shows very high phase stability, strongly reducing the need for active stabilisation. While in [16], the integrated laser source is an advantage in term of compactness and scalability, working with CW light, does not require RF modulation of laser diodes, simplifying the electronics design. A logical future direction of our demonstration is to use flip-chip bonding of VCSEL lasers to silicon photonics, as demonstrated recently [31]. Moreover our QRNG is directly integrable into

Optics EXPRESS

silicon devices, such as QKD systems demonstrated in [19,20]. Alternatively, our device could be integrated into multi-mode SOI devices, as the one demonstrated by Wang et al. [32], to provide a true random seed for device-independent randomness expansion. Finally we expect our QRNG to find applications whenever a low impact, high rate source of random numbers will be required in Silicon-on-Insulator devices.

Funding

H2020 European Research Council (ERC); PICQUE; BBOI; QUCHIP; US Army Research Office (ARO) (W911NF-14-1-0133); Engineering and Physical Sciences Research Council (EPSRC) (EP/M013472/1, EP/L024020/1, EP/M024385/1, EP/K033085/1).

Acknowledgments

The authors are grateful to M. Loutit, A. Murray and A. Crimp for technical support. JCFM (EP/M024385/1) and MGT (EP/K033085/1) acknowledge fellowship support from the EPSRC. During the completion of our manuscript we became aware of similar results present on the arXiv [33]. Underlying data are openly available at [34].