

Document downloaded from:

<http://hdl.handle.net/10251/84430>

This paper must be cited as:

Abellan, C.; Amaya Ocampo, WA.; Doménech Gómez, JD.; Muñoz Muñoz, P.; Capmany Francoy, J.; Longhi, S.; Mitchell, MW.... (2016). Quantum entropy source on an InP photonic integrated circuit for random number generation. *Optica*. 3(9):989-994.  
doi:10.1364/OPTICA.3.000989.



The final publication is available at

<http://dx.doi.org/10.1364/OPTICA.3.000989>

Copyright Optical Society of America

Additional Information

# A quantum entropy source on an InP photonic integrated circuit for random number generation

Carlos Abellan,<sup>1,2</sup> Waldimar Amaya,<sup>1</sup> David Domenech,<sup>3</sup> Pascual Muñoz,<sup>3,4</sup>  
Jose Capmany,<sup>3,4</sup> Stefano Longhi,<sup>5</sup> Morgan W. Mitchell,<sup>1,6</sup> and Valerio Pruneri<sup>1,6</sup>

<sup>1</sup>ICFO - Institut de Ciències Fotoniques, The Barcelona Institute of Science and Technology, 08860 Castelldefels (Barcelona), Spain

<sup>2</sup>Corresponding author: carlos.abellan@icfo.es

<sup>3</sup>VLC Photonics S.L. Cami de Vera s/n, Edificio 9B

<sup>4</sup>ITEAM Research Institute, Universitat Politècnica de Valencia, Spain

<sup>5</sup>Dipartimento di Fisica and Istituto di Fotonica e Nanotecnologie del CNR, Politecnico di Milano, Milan (Italy)

<sup>6</sup>ICREA - Institució Catalana de Recerca i Estudis Avançats, 08015 Barcelona, Spain

Random number generators are essential to ensure performance in information technologies, including cryptography, stochastic simulations and massive data processing. The quality of random numbers ultimately determines the security and privacy that can be achieved, while the speed at which they can be generated poses limits to the utilisation of the available resources. In this work we propose and demonstrate a quantum entropy source for random number generation on an indium phosphide photonic integrated circuit made possible by a new design using two-laser interference and heterodyne detection. The resulting device offers high-speed operation with unprecedented security guarantees and reduced form factor. It is also compatible with complementary metal-oxide semiconductor technology, opening the path to its integration in computation and communication electronic cards, which is particularly relevant for the intensive migration of information processing and storage tasks from local premises to cloud data centres.

<http://dx.doi.org/10.1364/OPTICA.3.000989>

## I. INTRODUCTION

Random numbers (RNs) are essential to a wide range of applications, including secure communications to protect the transmission and storage of confidential data [1], massive data processing [2], and stochastic simulations [3, 4] for stock market predictions, decision making in engineering processes and Monte Carlo calculations of physical, chemical, nuclear and biological events. Pseudo- RNs can be generated through computational algorithms while true RNs can only be generated through physical processes [5]. Quantum mechanical processes are the best guarantee for offering high-performance without compromising security and privacy. So far, several quantum entropy sources (QES) have been proposed for quantum random number generation (QRNG), including single photon splitting [6], homodyne detection of the vacuum field [7], and phase diffusion (PD) in semiconductor lasers [8, 9]. To date, PD-QRNGs have achieved the highest bit rates [10–12], up to 68 Gb/s [12], and passed severe random tests [13]. However, so far, PD-QRNGs have been realized with discrete optical components, often leading to devices of large size.

Photonic integrated circuit (PIC) technology [14, 15] is a key ingredient for building scalable optical devices [16]. The telecommunication industry is a clear example, and already accounts for commercial products such as semiconductor lasers, 100 GHz photo detectors, and high-bandwidth optical interconnects and transceivers [17]. Recently, the quantum optics community is making rapid progress in leveraging PIC technology, offering

the possibility to build scalable quantum optics experiments. In the field of quantum computation, PIC technology in combination with additional bulk elements, such as lasers, is allowing for the development of novel experiments otherwise impossible using tabletop components. Some examples include quantum simulation [18] and quantum enhanced sensing [19]. Quantum key distribution (QKD) functionalities have been also integrated using Indium Phosphide technology [20] and a monolithically integrated QRNG, composed of a light-emitting-diode (LED) and a single-photon-avalanche-photodetector (SPAD), has been recently demonstrated at 1 Mb/s using Silicon (Si) photonics technology [21]. Si photonics is a promising candidate for building scalable optical applications due to the compatibility with the microelectronics industry. However, the impossibility of creating a Si laser source poses serious limitations to the level of integration and performance of the PIC.

In this work, we show a fully integrated quantum entropy source for random number generation on an InP platform (QES-PIC) using standard fabrication techniques only. The device is made possible by a new design using two-laser interference and heterodyne detection, allowing QRNG rates in the Gb/s regime. We observe high interference visibility during long execution runs as well as superior temperature stability when compared to the bulk implementation of the same scheme. Also, using the Lang-Kobayashi rate equations model, we study in detail the dynamics of the two integrated lasers. We find conditions for operating the two-lasers with a negligible coupling effect, and provide an accurate description and modeling of the strong thermal

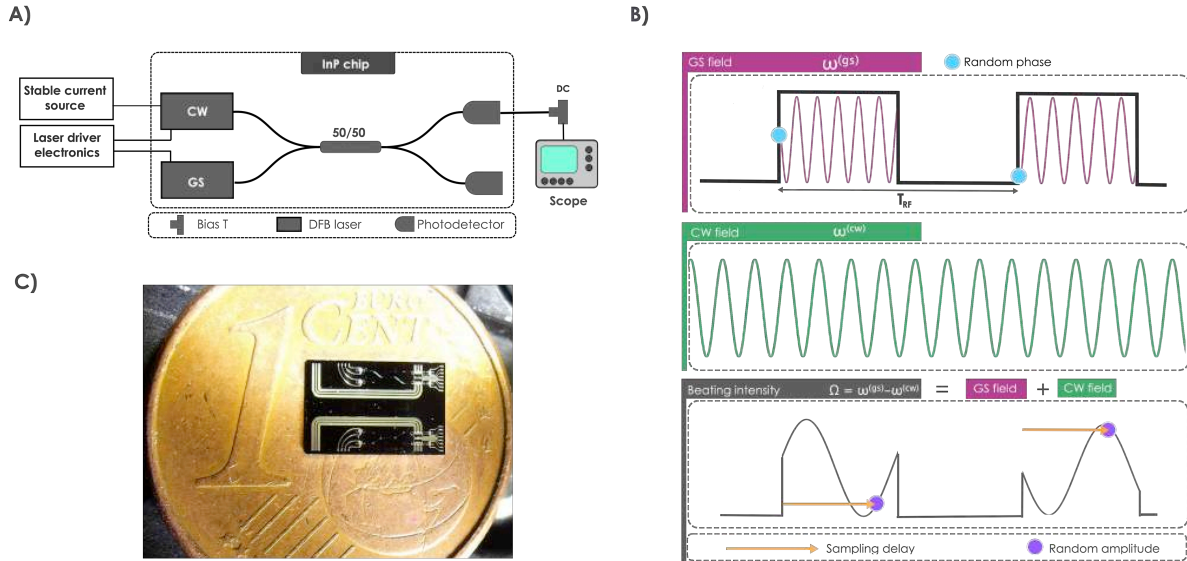


Figure 1. (a) Schematic of the quantum random number generator photonic integrated circuit (QRNG-PIC) based on two-laser interference. The two distributed feedback (DFB) lasers are biased with a current driver, one of them operating in continuous wave (CW) while the other one is periodically gain switched (GS) using an external RF generator. The temperature of the entire chip is controlled through a Peltier element while that of the area including one of the lasers is locally changed by a stable current source. The outputs from the two lasers are combined and interfered in a 2x2 multimode interference (MMI) coupler and two 40 GHz photodiodes (PDs) are placed at the output of the coupler. The detected signal is sent to a fast oscilloscope. (b) Principle of operation: optical pulses from a GS laser interfere with a CW laser generating an interference modulation whose frequency is equal to the difference of the two lasers' frequencies. The random phase of the GS laser pulse produces a random phase of the interference oscillation that can be properly sampled into a random amplitude. In this way, after digitization, one can extract one sample per GS pulse. (c) Microscope image of the PIC on a 1 Euro cent background. Two QRNG-PICs are printed on each chip.

chirp observed in the InP distributed feedback (DFB) lasers.

## II. EXPERIMENT

As illustrated in Fig. 1(A), we introduce a new QES scheme that combines two DFB lasers on the same chip. The first laser is operated in gain switching (GS) mode while the second one in continuous wave (CW) mode. By modulating continuously the GS laser from below to above threshold, optical pulses with nearly identical waveforms and completely randomized phases are generated. Then, by beating the GS and CW (the local oscillator) lasers through a multimode interference (MMI) coupler, an intensity oscillation forms with a beating frequency equal to the difference of the two lasers' frequencies, which can be detected by a photodetector (PD), see Fig. 1(B). Being  $i^{(CW)}$  and  $i^{(GS)}$  the intensities from the CW and the GS lasers respectively, we can write the total intensity at the output of the MMI (see supplementary material) as

$$i_T(t) = i_S(t) + 2i_P(t) \cos \left( \int_0^t d\xi \Omega_C(\xi) + \Delta\phi \right) \quad (1)$$

where  $i_S(t) \equiv i^{(CW)} + i^{(GS)}$  is the sum of the intensities from the two lasers,  $i_P(t) \equiv (i^{(CW)}i^{(GS)})^{1/2}$  the geometric mean,  $\Delta\phi = \phi^{(CW)} - \phi^{(GS)}$  the phase difference between the two lasers fields, and  $\Omega_C(t) = \Omega - \beta(t)$  the frequency detuning as a function of time. We introduced  $\beta(t) = \beta_0 t$  phenomenologically to account for frequency chirp arising from fast thermal effects in the directly-modulated laser [22]. Here,  $\Omega$  represents the initial frequency detuning between the two lasers. As illustrated in Fig. 1(B), the resulting signal corresponds to a train of pulses in which the amplitude of each pulse oscillates at  $\int_0^t d\xi \Omega_C(\xi)$  with a random phase  $\Delta\phi$  (for simplicity,  $\beta_0 = 0$  in the illustration). Finally, after the MMI coupler, a photodetector converts the optical signal into the electrical domain and random numbers are obtained by taking one sample per period.

A microscope image of the two laser QES-PIC is shown in Fig. 1(C). The chip was placed on top of a Peltier controller and its temperature was maintained at 25° with variations below 0.1°. The first DFB laser, with a bias of 10 mA, was operated in GS mode by superimposing a 100 MHz modulation from an Anritsu MP1800A pulse generator through a bias tee port. We chose this relatively low modulation frequency to capture properly the dynamics of the interference pattern within the GS pulse. However, modulation frequencies

up to 2 GHz are within immediate reach, allowing for 10s of Gb/s raw generation rates using current analog-to-digital conversion technologies, these being only limited by the stabilization time of the build-up dynamics of the laser intensity. The CW laser was operated by applying a constant 30 mA current. The beating signal was detected by an on-chip 40 GHz photodetector and digitized with a 20 GHz and 50 GSa/s real-time scope (Digital Phosphor Oscilloscope Tektronix DPO72004C), providing a temporal resolution of 20 ps to analyse the beat-note.

The central frequency of the two lasers could be independently tuned by injecting a constant current from a stable source Keithley 2401 through a metallic contact on the grating structure. The heating effect changed the average refractive index of the grating and consequently the Bragg condition, thus the operating frequency (wavelength) of each laser. By tuning these currents, the detuning frequency between the two lasers could be reduced and brought within the detection bandwidth.

### III. RESULTS

#### A. Modelling

When the frequencies of the two lasers are tuned closed to each other, back reflections from the MMI coupler can give rise to phase (frequency) locking effects. This phenomenon can be explained on the basis of the general mechanism of Adler's synchronisation of two coupled nonlinear oscillators [23–25] and modeled by the Lang-Kobayashi rate equation analysis for two mutually-coupled semiconductor lasers [26–28]. Indicating by  $\kappa$  the effective coupling rate between the two laser cavities and by  $\Omega$  the frequency detuning between the two bare longitudinal modes of the uncoupled cavities, neglecting delay effects it is known in simple Adler's theory of synchronisation that frequency locking occurs for  $|\Omega| < 2\kappa$  [23]. A more accurate analysis can be gained from rate equation analysis. We model the coupled laser system with rate equations for the normalised complex slowly varying envelope of the optical fields  $E_{1,2}$  and the normalised inversions  $N_{1,2}$  using standard Lang-Kobayashi rate equations [26–28], which in dimensionless form read [28]

$$\dot{E}_1 = \gamma(1 + i\alpha)N_1E_1 + \kappa \exp(i\psi)E_2(t - \tau_d) + \sqrt{R_1}\xi_1(t) \quad (2)$$

$$\dot{E}_2 = \gamma(1 + i\alpha)N_2E_2 + \kappa \exp(i\psi)E_1(t - \tau_d) + i[\Omega + \beta(t)]E_2\sqrt{R_2}\xi_2(t) \quad (3)$$

$$\tau\dot{N}_1 = P_1 - N_1 - (1 + 2N_1)|E_1|^2 \quad (4)$$

$$\tau\dot{N}_2 = P_2 - N_2 - (1 + 2N_2)|E_2|^2 \quad (5)$$

In Eqs. (2-5),  $\alpha$  is the linewidth enhancement factor,  $\gamma$  is the photon decay rate in the two laser cavities,  $\tau$  is

the carrier lifetime,  $\kappa$  is the coupling rate due to spurious optical feedback,  $\tau_d$  and  $\psi$  are the time and phase delays of optical feedback,  $P_{1,2}(t)$  are the normalized pump parameters of the two lasers, and  $\Omega$  is the difference between the oscillating frequencies of the two uncoupled lasers. The normalized pump parameter  $P$  is given by  $P = G_N N_0(x - 1)/2$ , where  $G_N$  is the differential gain,  $N_0$  is the current density at threshold, and  $x = J/J_{th}$  is the actual pumping current density normalized to its threshold value. Spontaneous emission is modeled by Langevin forces describing a Gaussian white noise process  $\xi(t)$  with zero mean and correlations given by  $\langle \xi_R(t)\xi_R(t') \rangle = \langle \xi_I(t)\xi_I(t') \rangle = \delta(t - t')$ , and  $\langle \xi_R(t)\xi_I(t') \rangle = 0$  [29]. For the laser operated with a carrier density not too far from its threshold value, the noise term becomes additive with a variance  $R = R_{sp}$ , where  $R_{sp}$  is the spontaneous emission variance [29].

To simulate the experimental results, we assume that the first laser is pumped with a constant current ( $P_1 = \bar{P}_1$ ), whereas the second laser is periodically GS from below to above threshold with a current pulse  $P_2(t)$ . In the simulations, the normalized pump parameter for the second laser in each modulation cycle is assumed to be of the form

$$P_2(t) = \bar{P}_2 \left\{ -\frac{1}{2} + \frac{3}{2} \exp[-(t/\Delta\tau)^{2M}] \right\}, \quad (6)$$

where  $\bar{P}_2$  is the peak of normalized pump current,  $\Delta\tau$  the current pulse duration and  $M$  the super-Gaussian parameter.

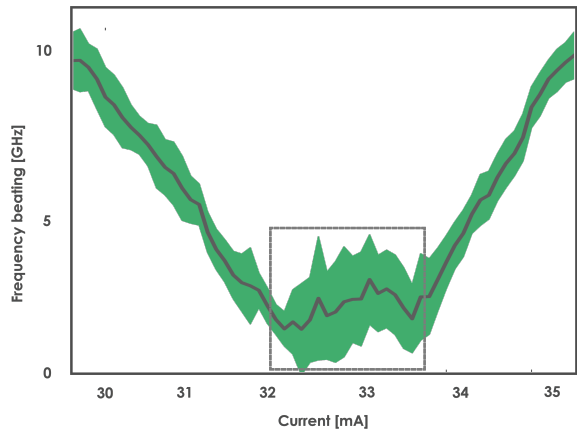


Figure 2. Beat-note frequency at the output of the MMI measured by sweeping one of the integrated lasers while keeping the other one constant in the low-loss QRNG-PIC. The beat-note frequency can be continuously tuned by current control for large detuning frequencies, whereas for small detuning frequencies phase (frequency) locking may occur (grey square), leading eventually to disappearance of the oscillation.

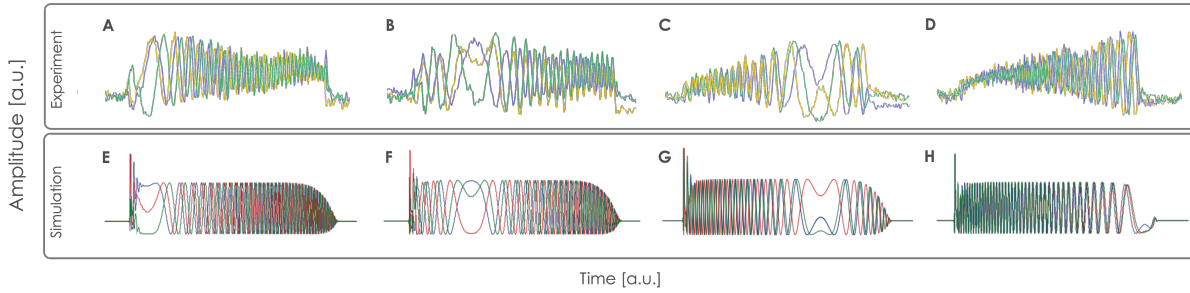


Figure 3. Temporal dynamics of the beating between the two lasers forming the high-loss QRNG-PIC and comparison with numerical results. (A-D) Experimental data with different temperature settings (currents). Chirp due to thermal effects and attenuation of beating amplitude due to the bandwidth limit of the detection electronics are evident. (E-H) Numerical results with initial detuning frequencies set to fit the experimental observations in (a).

## B. Numerical simulation and experimental parameters

In the experiments we used two PICs: a high waveguide propagation-loss PIC that ensures absence of significant back reflection from the CW into the GS laser and another one with a similar structure but lower loss. In the lower loss PIC, back-reflections at the MMI interface eventually induce phase-locking effects, preventing the generation of random oscillations. The coupling constant  $\kappa$  can be estimated from the locking region of the two lasers in the low-loss chip, see Fig. 2, and is given by  $\kappa = 5 \text{ ns}^{-1}$ . With such a high coupling constant, the Langevin forces entering in Eqs. (2-5) are too weak and therefore phase locking is observed in spite of spontaneous emission noise.

To obtain the QRNG functionality, it is therefore mandatory to reduce the feedback arising from spurious reflections at the MMI coupler. This goal was simply achieved by increasing the optical losses of the bus waveguides ( $\sim 15 \text{ dB/mm}$ ). As a result, the coupling rate  $\kappa$  between the two laser cavities is reduced by about  $\sim 30 \text{ dB}$  from the previously discussed low-loss PIC. For this high-loss PIC, the coupling, if any, is very weak, and thus phase randomization due to quantum noise prevails over phase locking, as shown in Fig. 3. Parameter values used in the simulation are shown in Table I. We use the instantaneous coupling approximation [27], i.e. the delay  $\tau_d$  can be neglected when solving Eqs. (2-3), since the time delay and coupling rate of feedback satisfy the constraint  $\tau_d \kappa < 1/\sqrt{1 + \alpha^2}$ . On the other hand, the phase delay  $\psi$  is difficult to estimate owing to its strong sensitivity to length changes over one wavelength; as a matter of fact it can be considered as an independent variable [24, 25]. Nevertheless, for parameter values that apply to our experimental conditions, a change of the phase delay, e.g. from  $\psi = 0$  to  $\psi = \pi/2$ , does not introduce substantial changes in the beating dynamics.

Table I. The value of the chirp rate  $\beta_0$  has been chosen to qualitatively fit the experimental results and is consistent with the data reported in [22]. The delay time  $\tau_d$  is determined by the optical path between the laser output facet and the MMI coupler.

Parameter	Symbol	Value
Linewidth enhancement factor	$\alpha$	2
Carrier lifetime	$\tau$	1 ns
Photon decay rate	$\gamma$	$150 \text{ ns}^{-1}$
Feedback delay time	$\tau_d$	20 ps
Normalised pump parameter	$\bar{P}_1 = \bar{P}_2$	8
Current pulse duration	$\Delta\tau$	5 ns
Super-Gaussian parameter	$M$	5
Chirp rate	$\beta_0$	$2\pi \times 1 \text{ MHz/ns}$
Spontaneous emission rate	$R_{sp}$	$2 \times 10^{-4} \text{ ps}^{-1}$

## C. Measuring the beating dynamics

For both the high- and low-loss PICs, the optical pulses of the GS laser were strongly chirped due to thermal effects, yielding a frequency-varying oscillation of the beating pattern, as depicted in Fig. 3. As a result, a nearly-zero-detuning (NZD) region was observed within the optical pulses when the chirped frequency of the GS laser coincides with the stable frequency of the CW laser. The position of the NZD region depends on the initial frequency separation between the GS and the CW emission lines. When both lasers were initially close (far) in frequency, the NZD region occurred at the beginning (end) of the pulse, see Fig. 3. In the high (15 dB/cm) waveguide loss PIC, the interference amplitude within the NZD region changed from pulse to pulse, a clear signature that phase noise dominated. Instead, in the low loss PIC (2 dB/cm), back reflection from the CW into the GS laser was not negligible and phase locking between the two lasers was observed. In this case, the interference amplitude in the NZD region did not appreciably change from pulse to pulse.

In the experiment, the NZD region was tuned at the end of the pulse (see Fig. 3(D)) maximizing the detuning frequency between the two lasers so as to reduce residual phase locking effects, if any.

#### D. PIC stability and performance

From a practical point of view, long-term stability of the scheme is a critical aspect. As we are interfering signals from two independent lasers, intrinsic phase noise and temperature drifts can severely affect the performance. In Fig. 4(A), we plot the histogram for 6 data sets with 200,000 samples each. The digitised signal was distributed according to the arcsine probability distribution function because of the initial random phase [10, 11] and the digitisation frequency asynchronous with respect to the beating (detuning) frequency. High stability was observed between acquisitions taken during 14 hrs., confirming the robustness of the two-laser scheme QES-PIC. Instead, a similar implementation with discrete (bulk) components suffered from slow temperature drifts (see supplementary material for details on the bulk implementation and corresponding experimental results). The higher stability of the PIC over the bulk design was mainly associated to the fact that the two lasers are closely located in a region with uniform temperature.

In Fig. 4(B), we show the autocorrelation function  $\Gamma_x(k) \equiv \langle x_i x_{i+k} \rangle - \langle x_i \rangle^2$  of a sequence of  $n = 10^7$  samples up to a delay of 500 samples. For such sequence length, the statistical uncertainty due to finite size effects is  $3.16 \times 10^{-4}$ . Except for the  $d = 1$  coefficient, which is significantly larger than the statistical noise sensitivity, all the other coefficients fall within the statistical noise level and pass the D'Agostino-Person's normality test with a  $p$ -value of 0.18. We attribute the larger correlation at  $d = 1$  to limitations in the direct modulation of the DFB LD in the experiment, leading to residual photons in the cavity from pulse to pulse. Samples from the higher loss PIC were acquired using a 50 GSa/s resolution and 20 GHz bandwidth real time scope, followed by a 30 dB RF amplifier. The amplifier introduced noise at several frequency bands, so we employed a 30 MHz high pass-band digital filter to remove low-frequency components. In addition, we want to assess the quality of the QES, so we want to analyze the correlation of the beat signal only. For doing so, we assume the noise is independent of our signal and calculate  $\Gamma_x = \Gamma_y - \Gamma_n$ , where  $\Gamma_y$  corresponds to the autocorrelation of samples taken within the GS pulse, and  $\Gamma_n$  to samples taken outside the GS pulse.

#### IV. DISCUSSION

The production of application-ready random numbers from the QES requires a randomness extraction

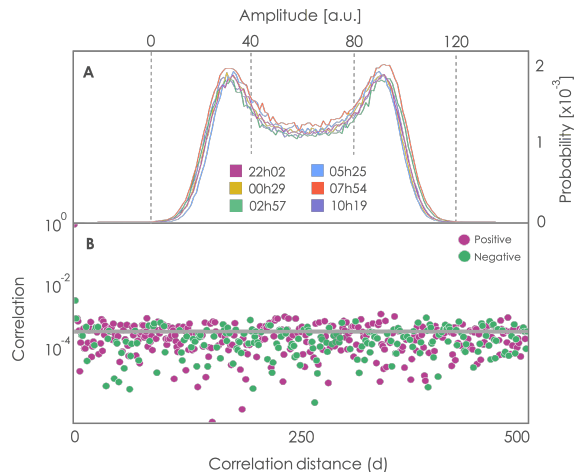


Figure 4. Statistics on the output of the QES-PIC. (a) Histograms on 6 sets of 200,000 samples each taken during 14 hrs, confirming stable operation of the QES-PIC device. (b) Auto-correlation function for  $10^7$  random samples taken with a 20 GHz scope and 50 GSa/s. Magenta (green) circles correspond to positive (negative) correlation coefficients.

stage [30]. In real QRNG devices, untrusted noise degrades (corrupts) the purity of the randomness associated to quantum processes. The application of proper randomness extractors allows to eliminate corruption of the quantum signal [30]. Random extraction requires (i) the estimation of the amount of available min-entropy from the QES, taking into account electronic noise, memory effects and digitization noise [31], and (ii) an appropriate hashing of the data after digitization. Thus, a full QRNG solution that includes both the QES and the electronics (including the digitizer) is required before any meaningful entropy estimate can be derived. However, the statistical data reported in Fig. 4 (correlation and distribution) already confirms the high randomness quality, as it is comparable to the raw data obtained with previously demonstrated bulk architectures, in which large entropy rates have been reported employing different digitization strategies in complete PD-QRNG solutions [13, 31]. With respect to the post-processing algorithm, field-programmable-gate-arrays (FPGAs) can be used for real-time randomness extraction above 1 Gb/s [32] for high-performance applications, while for lower-end applications, such as consumer electronics, the central processing unit (CPU) can sustain up to several Mb/s [33].

#### V. CONCLUSION

We have presented an ultra-fast quantum entropy source on a photonic integrated circuit (QES-PIC) for use in quantum random number generation (QRNG). The resulting device shows high performance, including

bit rate, degree of randomness (low correlation values) and stability, in a miniaturised geometry that also integrates the receiver. Considering its small footprint and the possibility for hybrid integration with CMOS electronics, the proposed QES-PIC has the potential to become a future functionality in computer and communication cards, especially for cryptography and stochastic simulations. The high level of miniaturisation may even make the integration of the QES-PIC device in smartphones and tablets possible.

#### FUNDING INFORMATION

European Research Council project AQUMET, European Union Project QUIC (Grant Agreement No.

641122), Spanish MINECO under the Severo Ochoa programme (Grant No. SEV-2015-0522), project EPEC (Grant No. FIS2014- 62181-EXP), project Qu-CARD (SRTC1400C002844XV0), Catalan AGAUR 2014 SGR Grants No. 1295 and No. 1623, the European Regional Development Fund (FEDER) Grant No. TEC2013-46168-R, and by Fundació Privada CELLEX.

#### ACKNOWLEDGMENTS

We thank M. Jofre and M. Curty for stimulating discussions on the optical design and R. Baños for laboratory assistance.

See Supplement 1 for supporting content.

- 
- [1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.* **28**, 656–715 (1949).
- [2] S. Brin and L. Page, "The anatomy of a large-scale hypertextual Web search engine," *Computer networks and ISDN systems* **30**, 107–117 (1998).
- [3] M. Mascagni, Y. Qiu, and L. Y. Hin, "High performance computing in quantitative finance: A review from the pseudo-random number generator perspective," *Monte Carlo Methods and Applications* **20**, 101–120 (2014).
- [4] T. H. Click, A. Liu, and G. A. Kaminski, "Quality of random number generators significantly affects results of Monte Carlo simulations for organic and biological systems," *Journal of Computational Chemistry* **32**, 513–524 (2011).
- [5] J. Von Neumann, "Various techniques used in connection with random digits," *National Bureau of Standards Applied Math Series* **12**, 16–38 (1951).
- [6] J. G. Rarity, P. Owens, and P. R. Tapster, "Quantum random-number generation and key sharing," *J. Mod. Optics* **41**, 2435–2444 (1994).
- [7] C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Maurer, U. L. Andersen, C. Marquardt, and G. Leuchs, "A generator for unique quantum random numbers based on vacuum states," *Nature Photon.* **4**, 711–715 (2010).
- [8] 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).
- [9] 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).
- [10] 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).
- [11] Z. L. Yuan, M. Lucamarini, J. F. Dynes, B. Fröhlich, A. Plews, and A. J. Shields, "Robust random number generation using steady-state emission of gain-switched laser diodes," *Appl. Phys. Lett.* **104**, 261112 (2014).
- [12] Y. Q. Nie, L. Huang, Y. Liu, F. Payne, and J. Zhang, "The generation of 68 Gbps quantum random number by measuring laser phase fluctuations," *Rev. Sci. Instrum.* **86**, 063105 (2015).
- [13] C. Abellán, W. Amaya, D. Mitrani, V. Pruneri, and M. W. Mitchell, "Generation of fresh and pure random numbers for loophole-free Bell tests," *Phys. Rev. Lett.* **115**, 250403 (2015).
- [14] M. J. R. Heck, J. F. Bauters, M. L. Davenport, J. K. Doylend, S. Jain, G. Kurczveil, S. Srinivasan, Y. Tang, and J. E. Bowers, "Hybrid Silicon Photonic Integrated Circuit Technology," *IEEE J. Selected Topics in Quantum Electronics* **19**, 6100117 (2012).
- [15] M. Smit, X. Leijtens, H. Ambrosius, E. Bente, J. van der Tol, B. Smalbrugge, T. de Vries, E.-J. Geluk, J. Bolk, R. van Veldhoven, L. Augustin, P. Thijs, D. D'Agostino, H. Rabhani, K. Lawniczuk, S. Stopinski, S. Tahvili, A. Corradi, E. Kleijn, D. Dzibrou, M. Felicetti, E. Bitincka, V. Moskalenko, J. Zhao, R. Santos, G. Gilardi, W. Yao, K. Williams, P. Stabile, P. Kuindersma, J. Pello, S. Bhat, Y. Jiao, D. Heiss, G. Roelkens, M. Wale, P. Firth, F. Soares, N. Grote, M. Schell, H. Debregeas, M. Achouche, J.-L. Gentner, A. Bakker, T. Korthorst, D. Gallagher, A. Dabbs, A. Melloni, F. Morichetti, D. Melati, A. Wonfor, R. Penty, R. Broeke, B. Musk, and D. Robbins, "An introduction to InP-based generic integration technology," *Semicond. Sci. Technol.* **29**, 083001 (2014).
- [16] I. A. Walmsley, "Quantum optics: Science and technology in a new light," *Science* **348**, 525–530 (2015).
- [17] A. Alduino, L. Liao, R. Jones, M. Morse, B. Kim, W.-Z. Lo, J. Basak, B. Koch, H.-F. Liu, H. Rong, M. Sysak, C. Krause, R. Saba, D. Lazar, L. Horwitz, R. Bar, S. Lit-ski, A. Liu, K. Sullivan, O. Dosunmu, N. Na, T. Yin, F. Haubensack, I.-w. Hsieh, J. Heck, R. Beatty, H. Park, J. Bovington, S. Lee, H. Nguyen, H. Au, K. Nguyen, P. Merani, M. Hakami, and M. Paniccia, "Demonstration of a High Speed 4-Channel Integrated Silicon Photonics WDM Link with Hybrid Silicon Lasers," in "Integrated Photonics Research, Silicon and Nanophotonics and Photonics in Switching," (Optical Society of America, 2010), p. PDIWI5.

- [18] M. Tillmann, B. Dakić, R. Heilmann, S. Nolte, A. Szameit, and P. Walther, "Experimental boson sampling," *Nature Photon.* **7**, 540–544 (2013).
- [19] J. Matthews, A. Politi, A. Stefanov, and J. L. O'Brien, "Manipulation of multiphoton entanglement in waveguide quantum circuits," *Nature Photon.* **3**, 346–350 (2009).
- [20] P. Sibson, M. Godfrey, C. Erven, S. Miki, T. Yamashita, M. Fujiwara, M. Sasaki, H. Terai, M. G. Tanner, C. M. Natarajan, R. H. Hadfield, J. O'Brien, and M. G. Thompson, "Integrated Photonic Devices for Quantum Key Distribution," in "CLEO: 2015," (Optical Society of America, 2015), p. FF1A.6.
- [21] A. Khanmohammadi, R. Enne, M. Hofbauer, and H. Zimmermann, "A Monolithic Silicon Quantum Random Number Generator Based on Measurement of Photon Detection Time," *IEEE Photon. J.* **7**, 1–13 (2015).
- [22] A. Zadok, H. Shalom, M. Tur, W. D. Cornwell, and I. Andonovic, "Spectral shift and broadening of DFB lasers under direct modulation," *IEEE Photon. Technol. Lett.* **10**, 1709–1711 (1998).
- [23] R. Adler, "A study of locking phenomena in oscillators," in "Proc. IEEE," (IEEE, 1973), p. 1380.
- [24] D. G. Aronson, E. J. Doedel, and H. G. Othmer, "An analytical and numerical study of the bifurcations in a system of linearly-coupled oscillators," *Physica D* **25**, 20 (1987).
- [25] D. G. Aronson, G. B. Ermentrout, and N. Kopell, "Amplitude response of coupled oscillators," *Physica D* **41**, 403 (1990).
- [26] R. Lang and K. Kobayashi, "External optical feedback effects on semiconductor injection laser properties," *IEEE J. Quantum Electron.* **16**, 347–355 (1980).
- [27] S. Yanchuk, K. R. Schneider, and L. Recke, "Dynamics of two mutually coupled semiconductor lasers: instantaneous coupling limit," *Phys. Rev. E* **69**, 056221 (2004).
- [28] H. Erzgräber, D. Lenstra, B. Krauskopf, and E. Wille, "Mutually delay-coupled semiconductor lasers: Mode bifurcation scenarios," *Opt. Express* **255**, 286–296 (2005).
- [29] A. Torcini, S. Barland, G. Giacomelli, and F. Marin, "Low-frequency fluctuations in vertical cavity lasers: Experiments versus Lang-Kobayashi dynamics," *Phys. Rev. A* **74**, 063801 (2006).
- [30] D. Frauchiger, R. Renner, and M. Troyer, "True randomness from realistic quantum devices," *arXiv* (2013).
- [31] M. W. Mitchell, C. Abellán, and W. Amaya, "Strong experimental guarantees in ultrafast quantum random number generation," *Phys. Rev. A* **91**, 012314 (2015).
- [32] A. Martin, B. Sanguinetti, C. C. W. Lim, R. Houlmann, and H. Zbinden, "Quantum random number generation for 1.25 GHz quantum key distribution systems," *J. Lightw. Technol.* **33**, 2855–2859 (2015).
- [33] B. Sanguinetti, A. Martin, H. Zbinden, and N. Gisin, "Quantum random number generation on a mobile phone," *Physical Review X* **4**, 031056 (2014).