We report an accelerated laser phase diffusion quantum entropy source with all non-laser optical and optoelectronic elements implemented in silicon photonics. The device uses efficient and robust single-laser accelerated phase diffusion methods, and implements the whole quantum entropy source scheme including an unbalanced Mach-Zehnder interferometer with optimized splitting ratio, in a 0.5 mm × 1 mm footprint. We demonstrate Gbps raw entropy-generation rates in a technology compatible with conventional CMOS fabrication techniques.

© 2018 Optical Society of America

OCIS codes: (130.0130) Integrated optics; (230.3120) Integrated optics devices; (270.0270) Quantum optics.

http://dx.doi.org/10.1364/optica.XX.XXXXXX

1. INTRODUCTION

On-demand generation of random numbers (RNs) is a key ingredient for fields as diverse as Monte Carlo simulations [1, 2], online gambling applications [3], decision making algorithms, cybersecurity [4, 5], and even tests of fundamental physics [6–9]. Although pseudo-RNs can be easily generated using computational algorithms, true RNs can only be created using physical processes [5, 10]. Quantum entropy sources (QESs) make use of the intrinsic randomness of quantum mechanics, creating strings of random bits. Several implementations of QESs have been demonstrated, including splitting of single photons [11, 12], photon arrival time [13], vacuum fluctuations [14], laser chaos [15, 16], and phase diffusion (PD) in laser diodes [17–21]. In particular, PD-QESs have been shown to achieve high bit rates and offer strong randomness guarantees [6].

For future devices it is desirable to scale down these bulky technologies into integrated devices. Recently, an integrated QES using a light emitting diode (LED) and a single-photon avalanche photodetector (SPAD) achieved 1 Mbps bit rates [22]. PD-QESs have the potential to achieve several orders of magnitude higher rates as they use conventional photodetectors instead of SPAD. A PD-QES in an indium phosphide (InP) integrated circuit was demonstrated with Gbps rates [23]. Implementation in silicon photonics, which we show here, allows direct integration with conventional complementary metal oxide semiconductor (CMOS) electronics, enabling QES deployment in the most advanced semiconductor industry.

In this work we demonstrate a PD-QES on a Si chip using an integrated unbalanced Mach-Zehnder interferometer (uMZI) scheme. The laser component cannot be directly implemented in Si photonics, although hybrid technologies, like Germanium-on-Silicon [24] or 2D materials [25] have shown the potential for full PD-QES integration onto a single chip. Here the device is driven by an external DFB laser operated in gain-switching (GS) mode to generate pulses with equal amplitudes and random initial phases. These pulses are then interfered in the uMZI, thus creating a train of pulses with random amplitudes that are measured in a high bandwidth integrated photodetector (PD). The scheme shows high stability over time and can potentially deliver Gbps bit rates with appropriate digitization components.

2. EXPERIMENT

Figure 1 shows a schematic of the experimental set-up and an image of the Si chip containing QES devices. The Si chip implements both the interferometry and photodetection elements of the PD-QES strategy. The laser component is interfaced to the chip by a grating coupler (GC). A single-frequency (λ = 1550 nm) DFB laser is operated in GS mode, with a mean drive current of 14 mA and a sinusoidal modulation at 1 GHz, applied via a bias-tee. As the laser threshold is 10 mA, this takes the laser above and far below threshold on each cycle, producing a train of linearly-polarized optical pulses of duration ∼300 ps.

Due to phase diffusion, subsequent pulses have random relative phases, while also having the same waveforms. In order to couple the pulses into the Si chip, the laser output is directed via an SMF towards a GC at 10° incidence using a 6-axis micropositioner. A polarization controller (PC) is used to adjust the input polarization to minimize the coupling losses due to
the GC, which were estimated to be \( \sim 7 \) dB by measuring the transmission through a straight waveguide.

In the chip, a first multimode interference coupler (MMI) splits the input light, with a power-splitting ratio of 0.02:0.98, to the two arms of an uMZI, in order to compensate the losses introduced by the longer path. The interference signal is detected using an integrated photodetector and analyzed with a real-time oscilloscope.

\[ t_l/t_s = \exp(x \Delta l) \]  

(1)

here \( x \sim 0.56 \text{ cm}^{-1} \) is the attenuation coefficient of the Si waveguide and \( \Delta l = 6.9 \text{ cm} \) is the relative path difference of the uMZI, given by \( \Delta l = \tau c/n_g \), where \( \tau = 1 \text{ ns} \) is the pulse repetition rate and \( n_g \sim 4.3 \) is the effective group refractive index of the Si waveguide. This implies a relative attenuation by a factor of \( \sim 50 \), compensated by the first MMI and thus equalizing the field strength reaching the detector, while the path length difference introduces a delay of 1 ns that creates the conditions for temporal overlap of subsequent pulses. Careful control of these parameters is crucial in order to obtain high interference visibility. Finally, the interfered pulses are detected by a fast (10 GHz) on-chip photodiode (responsivity \( \sim 0.7 \text{ A/W} \)) and sent to a 4 GHz real-time oscilloscope via a bias-tee.

**3. DISCUSSION**

As described in [6], the power detected by the integrated photodiode is given by

\[ P_{\text{det}}(t) = P_l(t) + P_l(t + \tau) + 2V \sqrt{P_l(t)P_l(t + \tau)} \cos(\Delta \theta + \Delta \phi) \]  

(2)

where \( P_l(t) \) is the instantaneous laser power at time \( t \), \( \tau = 1 \text{ ns} \) is the pulse repetition period, \( V \) is the interference visibility, \( \Delta \theta \) is the relative phase between subsequent pulses, and \( \Delta \phi \) is the optical phase acquired in the uMZI. Due to strong phase diffusion in the time below threshold, the statistical description of \( \Delta \phi \) is, to a very good approximation, random, i.e., uniformly distributed on \( [0, 2\pi] \). As a result, the cosine of \( \Delta \theta \) follows a bimodal distribution [6], irrespective of \( \Delta \phi \).

By measuring the statistics of the electrical signal when the laser is below threshold (orange curve in Figure 2) one can also obtain information about the overall noise of the system, which ultimately determines the quality of the device. Figure 2 shows the observed distribution of output powers. The optical and electronic noises produce a monomodal distribution for the equivalent input power, whereas the interference process produces a strongly bimodal distribution, reflecting the arcsine distribution expected from the phase diffusion process smoothed by convolution with the electronic noise distribution.
interferometry and detection components. Up to 20 PD-QESs can be integrated on a single chip with a footprint of only $4\times 7.5$ mm$^2$, with a single PD-QES footprint of 0.5x1 mm$^2$. The amplitude of the interfered pulses follows a smoothed arcsine distribution, as expected for PD-QESs, with a visibility of $V = 0.74$ and random $\Delta\theta$. Also, we have introduced a method to qualitatively verify the correlation in the real-time oscilloscope without any need of offline post-processing.

Finally, the scheme could easily achieve tens of Gbps bit rates by using shorter uMZIs and thus faster modulation frequencies. This would in turn increase the SNR due to the decreased attenuation of the pulses inside the uMZI and allow integration of the PD-QES in chips with a smaller footprint.

5. FUNDING INFORMATION

Valuni Kipos; Fundació Privada Cellex; CERCA Programme/Generalitat de Catalunya; Spanish Ministry of Economy and Competitiveness, through the ‘Severo Ochoa’ Programme for Centres of Excellence in R&D (SEV-2015-0522) and OPTO-SCREEN (TEC2016-75080-R). European Research Council (ERC) project ERIDIAN (713682); European Union project QUIC (Grant Agreement no. 641122); Spanish MINECO projects MAQRO (Ref. FIS2015-68039-P); XPLICA (FIS2014-62181-EXP); Agència de Gestió d’Ajuts Universitaris i de Recerca (AGAUR) project (2014-SGR-1295);

REFERENCES

1. X. Cai and X. Wang, IEEE Signal Process. Mag. 24, 27 (2007).
2. T. H. Click, A. Liu, and G. A. Kaminski, J. Comput. Chem. 32, 513 (2011).
3. C. Hall and B. Schneier, “Remote electronic gambling,” in “Computer Security Applications Conference, 1997. Proceedings., 13th Annual,” (IEEE, 1997), pp. 232–238.
4. C. E. Shannon, Bell Syst. Tech. J. 28, 656 (1949).
5. A. Tajima, A. Tanaka, W. Maeda, S. Takahashi, and A. Tomita, IEEE J. Sel. Topics in Quantum Electron. 13, 1031 (2007).
6. C. Abellán, W. Amaya, D. Mitrani, V. Pruneri, and M. W. Mitchell, Phys. Rev. Lett. 115, 250403 (2015).
7. B. Hansen, H. Bernien, A. Dréau, A. Reiserer, N. Kalb, M. Blok, J. Ruitenberg, R. Vermeulen, R. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, R. Hanson, Nature 526, 682 (2015).
8. M. Giustina, M. A. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J.-Å. Larsson, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, J. Beyer, T. Gerrits, A. E. Lita, L. K. Shalm, S. W. Nam, T. Scheidl, R. Ursin, B. Wittman, A. Zeilinger, Phys. Rev. Lett. 115, 254001 (2015).
9. L. K. Shalm, E. Meyer-Scott, B. G. Christensen, P. Bierhorst, M. A. Wayne, M. J. Stevens, T. Gerrits, S. Glancy, D. R. Hamel, M. S. Allaman, K. J. Coakley, S. D. Dyer, C. Hodge, A. E. Lita, V. B. Verma, C. Lambrocco, E. Tortorici, A. L. Migdall, Y. Zhang, D. R. Kumor, W. H. Farr, F. Marsili, M. D. Shaw, J. A. Stern, C. Abellán, W. Amaya, V. Pruneri, T. Jennewein, M. W. Mitchell, P. G. Kwiat, J. C. Bienfang, R. P. Mirin, E. Knill, S. W. Nam, Phys. Rev. Lett. 115, 250402 (2015).
10. J. Von Neumann, Appl. Math Ser. 12, 36 (1951).
11. J. Rarity, P. Owens, and P. Tapster, J. Mod. Opt. 41, 2435 (1994).
12. T. Jennewein, U. Aichelburger, G. Weihs, H. Weinfurter, and A. Zeilinger, Rev. Sci. Instr. 71, 1675 (2000).
13. M. Wahl, M. Leifgen, M. Berlin, T. Röhlicke, H.-J. Rahn, and O. Zilinger, Appl. Phys. Lett. 98, 171105 (2011).
14. C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Maurer, U. L. Andersen, C. Marquardt, and G. Leuchs, Nature Photon. 4, 711 (2010).
15. A. Argyris, S. Deligiannidis, E. Pikas, A. Bogris, and D. Syrvidis, Opt. Express 18, 18763 (2010).
16. K. Ugajin, T. Terashima, K. Iwakawa, A. Uchida, T. Harayama, K. Yoshimura, and M. Inubushi, Opt. Express 25, 6511 (2017).
17. B. Qi, Y.-M. Chi, H.-K. Lo, and L. Qian, Opt. Lett. 35, 312 (2010).
18. M. Jofre, M. Curty, F. Steinlechner, G. Anzolin, J. P. Torres, M. W. Mitchell, and V. Pruneri, Opt. Express 19, 20665 (2011).
19. C. Abellán, W. Amaya, M. Jofre, M. Curty, A. Acín, J. Capmany, V. Pruneri, and M. W. Mitchell, Opt. Express 22, 1645 (2014).
20. Z. Yuan, M. Lucamarini, J. Dynes, B. Fröhlich, A. Plews, and A. Shields, Appl. Phys. Lett. 104, 261112 (2014).
21. Y.-Q. Nie, L. Huang, Y. Liu, F. Payne, J. Zhang, and J.-W. Pan, Rev. Sci. Instr. 86, 063105 (2015).
22. A. Khanmohammadi, R. Enne, M. Hofbauer, and H. Zimmermanna, IEEE Photon. J. 7, 1 (2015).
23. C. Abellan, W. Amaya, D. Domenech, P. Muñoz, J. Capmany, S. Longhi, M. W. Mitchell, and V. Pruneri, Optica 3, 989 (2016).
24. R. E. Camacho-Aguilera, Y. Cai, N. Patel, J. T. Bessette, M. Romagnoli, L. C. Kimerling, and J. Michel, Opt. Express 20, 11316 (2012).
25. Y.-Q. Bie, G. Grosso, M. Heuck, M. M. Furchi, Y. Cao, J. Zheng, D. Bunandar, E. Navarro-Moratalla, L. Zhou, D. K. Efetov, T. Taniguchi, K. Watanabe, J. Kong, D. Englund, P. Jarillo-Herrero, Nature Nanotech. doi:10.1038/nnano.2017.209 (2017).
26. N. Nisan and A. Ta-Shma, J. Comp. Syst. Sci. 58, 148 (1999).
FULL REFERENCES

1. X. Cai and X. Wang, “Stochastic modeling and simulation of gene networks-a review of the state-of-the-art research on stochastic simulations,” IEEE Signal Processing Magazine 24, 27–36 (2007).

2. 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).

3. C. Hall and B. Schneier, “Remote electronic gambling,” in “Computer Security Applications Conference, 1997. Proceedings., 13th Annual,” (IEEE, 1997), pp. 232–238.

4. C. E. Shannon, “Communication theory of secrecy systems,” Bell System Technical Journal 28, 656–715 (1949).

5. A. Tajima, A. Tanaka, W. Maeda, S. Takahashi, and A. Tomita, “Practical quantum cryptosystem for metro area applications,” IEEE Journal of Selected Topics in Quantum Electronics 13, 1031–1038 (2007).

6. 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).

7. B. Hensen, H. Bernien, A. Dréau, A. Reiserer, N. Kalb, M. Blok, J. Ruitenberg, R. Vermeulen, R. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, R. Hanson, “Loophole-free bell inequality violation using electron spins separated by 1.3 kilometres,” Nature 526, 682–686 (2015).

8. M. Giustina, M. A. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J.-Å. Larsson, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, J. Beyer, T. Gerrits, A. E. Lita, L. K. Shalm, S. W. Nam, T. Scheidl, R. Ursin, B. Wittman, A. Zeilinger, “Signifcant-loophole-free test of bell?’s theorem with entangled photons,” Physical Review Letters 115, 250401 (2015).

9. L. K. Shalm, E. Meyer-Scott, B. G. Christensen, P. Bierhorst, S. J. Blair, M. A. Wayne, M. J. Stevens, T. Gerrits, S. Glancy, D. R. Hamel, M. S. Allman, K. J. Coakley, S. D. Dyer, C. Hodge, A. E. Lita, V. B. Verma, C. Lambropoulos, E. Tortorici, A. L. Migdall, Y. Zhang, D. R. Kumor, W. H. Farr, F. Marsili, M. D. Shaw, J. A. Stern, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, T. Jennewein, M. W. Mitchell, P. G. Kwiat, J. C. Bienfang, R. P. Mirin, E. Knill, S. W. Nam, “Strong loophole-free test of local realism,” Physical Review Letters 115, 250402 (2015).

10. J. Von Neumann, “Various techniques used in connection with random digits,” Appl. Math Ser 12, 36–38 (1951).

11. J. Rarity, P. Owens, and P. Tapster, “Quantum random-number generation and key sharing,” Journal of Modern Optics 41, 2435–2444 (1994).

12. T. Jennewein, U. Aichler, G. Weihs, H. Weinfurter, and A. Zeilinger, “A fast and compact quantum random number generator,” Review of Scientific Instruments 71, 1675–1680 (2000).

13. M. Wahl, M. Leifgen, M. Berlin, T. R??hlicke, H.-J. Kimlering, and J. Michel, “An electrically pumped germanium laser,” Opt. Express 20, 11316–11320 (2012).

14. Y.-Q. Bie, G. Grosso, M. Heuck, M. M. Furchi, Y. Cao, J. Zheng, D. Bunandar, E. Navarro-Moratalla, L. Zhou, D. K. Efetov et al., “A mote2-based light-emitting diode and photodetector for silicon photonic integrated circuits,” Nature Nanotechnology (2017).

15. N. Nisan and A. Ta-Shma, “Extracting randomness: A survey and new constructions,” Journal of Computer and System Sciences 58, 148 – 173 (1999).