Monolithic Integration of a Phase Noise Based Quantum Random Number Generator on InP platform

D. Alvarez-Outerelo(1), M. Troncoso-Costas(1), I. Roumpos(3,4), T. Chrysostomidis(3,4), V. Moskalenko (2), K. Vyrsokinos(3,4), F. J. Diaz-Otero(1)

(1) atlanTTic Research Center, University of Vigo, EI Telecommunication, Campus Universitario s/n, 36310 Vigo, Spain, fjdiaz@com.uvigo.es
(2) Bright Photonics, Horsten 1, 5612 AR Eindhoven
(3) School of Physics, Aristotle University of Thessaloniki, 54124, Thessaloniki, Greece
(4) Center for Interdisciplinary Research, 57001, Thessaloniki, Greece

Abstract We present the experimental characterization of a fully integrated InP-based quantum random number generator chip composed from a single gain switched DBR laser and two Mach Zehnder interferometers. We demonstrate high degree of randomness by testing the QRNG output in the NIST Statistical Test Suite.

Introduction

Quantum random generators (QRNGs) are devices or circuits that target the generation of random bits [1],[2],[3] with true randomness that cannot be hacked by external sources. They exploit the quantum nature of light for the generation of quantum numbers with multiple application in the areas of cybersecurity, banking, datacenters and telecommunications, gaming and lotteries, etc [4]. However, the demonstrated solutions so far are based on physical devices and systems with macroscopically observable parameters that vary dynamically randomly, such as the phase noise or intensity of a CW laser[1],[2],[3], or vacuum fluctuations [5],[6] of amplifiers' spontaneous emission effects[7]. Between these solutions, the schemes based on the generation and measurement of phase noise have numerous advantages over the other approaches, regardless of the targeted application, because they use standard components, they are fast, exhibit higher bit rate and are robust against amplitude and phase fluctuations [8]. Photonic Integration has vastly pushed lab demonstration of QRNGs, since light can be controlled in a more precise way with devices relying on a plethora of material platforms such as Si [9,10] and InP [11] with each one delivering pros and cons related to footprint, speed and power consumption.

In this work, we present the experimental results from the characterization of a QRNG based on the generation of random numbers by combining phase noise produced in a laser cavity and interferometry in an indium phosphide (InP) monolithic integrated photonic circuit [12].

The PIC is composed of a DBR laser followed by an Unbalanced Mach Zehnder Interferometer (UBMZI) for conversion of random phase to random amplitude and is capable to produce random numbers at 1.245GHz with a footprint of only 9mm^2 and power consumption of only 118 mW. Another balanced MZI (BMZI) in between is controlling the power going to each arm of the BMZI for maximum interference contrast at the output of the UBMI. Once characterized, the QRNG PIC is analysed and post processed in terms of randomness performance. The operating device shows high degree of randomness with low correlation values. It passes several standard statistical tests, becoming a good candidate for a future term security encryption application, where low power consumption, small size and high-bit rate could be needed

PIC description and Experimental Setup

The QRNG was fabricated in InP active-passive integration platform available through Smart

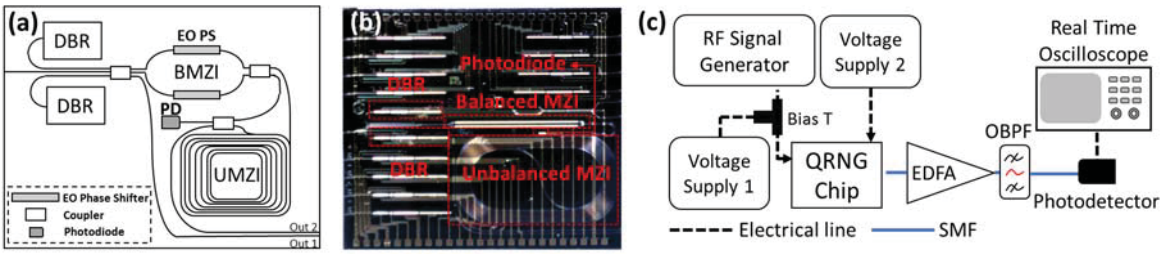

Fig. 1: (a) Schematic of the QRNG-PIC, (b) Image of the InP based chip fabricated by Smart Photonics operating as a source for quantum random number generation with identification of the key components (c) The experimental setup used to operate the QRNG.

2020 European Conference on Optical Communications (ECOC) | 978-1-7281-7361-0/20/$31.00 ©2020 IEEE | DOI: 10.1109/ECOC48923.2020.9333202

978-1-7281-7361-0/20/$31.00 ©2020 IEEE

Photonics foundry service. The schematic of the QRNG is shown in Figure 1(a) with the three main building blocks i.e. two DBR laser sources, a balanced MZI (BMZI) and an Unbalanced MZI (UMZI). The two lasers are connected to a 3x3 MMI with the third input providing an external port for characterization of the BMZI and the UMZI without restrictions from the in-chip lasers. The two out of the three output ports of the MMI are going to the two arms of the BMZI, while the third one is going to Output port 1 that allows direct characterization of the two lasers. The other Output port 2 is coming directly from the output port of the UMZI for off-chip signal evaluation.

The working principle of the proposed QRNG relies on generating optical pulses from a gain switched (GS) DBR laser that is biased slightly above the threshold. When the current modulation is deep enough, the laser reaches sub-threshold state between the pulses and in this case the phase of each pulse is defined by the randomness of amplified spontaneous emission. The random phase of the adjacent pulses is translated to random amplitude through the UMZI featuring a 65.4mm length difference between the two arms that results 12dB power difference between the two pulse trains before interfering at the output coupler. This power unbalance affects significantly the quality of the signal to noise ratio at the output of the chip and for this reason a BMZI with EO phase shifters on each arm is employed to control the power ratio that is going from the DBR laser to the two branches of the UMZI. The two outputs of the UMZI are connected to Output port 2 and to a on chip photodiode. However, due to the strong RF applied to the laser for the gain switching and the high losses from the circuit, the electrical cross-talk was very high and rendered non-functional the OE conversion from this PD that would allow the demonstration of QRNG from a single chip. Figure 1(b) present a microscope image of the chip highlighting the position and occupied area of all main components.

The evaluation of the circuit was performed with the experimental setup of Figure 1(c) utilizing Output Port 2. The chip was mounted on thermally stabilized vacuum chuck with the temperature set at 23°C. The threshold of the DBR laser was measured with P-I measurement at 12 mA with signal collected from Output port 1 coming directly from the 3x3 coupler. The other laser connected to the MMI exhibited similar threshold, but provided slightly lower output power and was discarded for further evaluation.

Optimum GS regime for highest signal randomness was observed when an RF signal generator provided 21 dBm of power at 1.245 GHz frequency and biasing conditions of the top laser in Figure 1(a) was 18mA and 0.98 V coming from Voltage Supply 1. The RF and DC signals were mixed with a Bias T of 18 GHz bandwidth inducing 1dB loss and then applied to the laser with a GSG RF probe. Voltage supply 2 was used to tune the power at the outputs of the BMZI that is consisted by two XX mm long DC EO phase shifters. After detailed characterization it was found that the best signal to noise ratio was achieved when the top phase shifter was reversed biased with -5.7V. In these conditions the output power measured directly at output port 2 was -40.7 dBm, that was too low for direct post processing. So, a low noise Erbium-doped fiber preamplifier (EDFA) followed by a 1nm tunable optical bandpass filter (OBPF) was placed at the output of the chip that provided 0 dBm output power. The amplified signal was then injected to a 70 GHz photodetector for the OE conversion and subsequently monitored with a real time oscilloscope of 33 GHz bandwidth at 80 GSa/s sampling rate. In total 4 Msamples were recorded for the applied settings for further post processing. With these settings the total power consumption of the chip is calculated to 118 mW.

Analysis and post processing

A process of peak detection was made on the results from the experiment by choosing the highest value of the measurements corresponding to one pulse collision. The analysis and post processing of the obtained sequence is divided in two main topics: the analysis of the decimal sequence, and the conversion to binary, randomness extraction, and statistical analysis of the final sequence.

The decimal sequence was first tested to check the assumption of Gaussian distribution. This was done both by graphical, histogram (Figure 2) and Q-Q plot, and quantitative means. The normality tests used, and the percentage of times they were passed, are Pearson's chi-squared test (97%), Kolmogorov-Smirnov test (96%), Lilliefors test (97%) and Jarque-Bera test (96%). The decimal sequence was also checked for hidden patterns

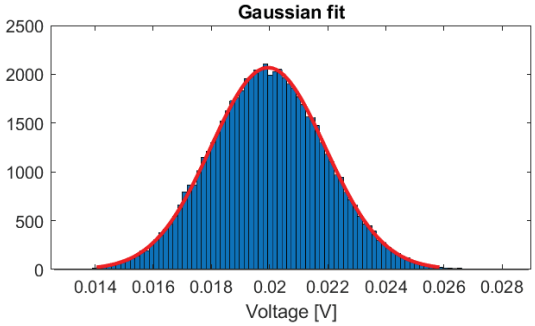

Fig. 2: Histogram and gaussian fit of the measured sequence.

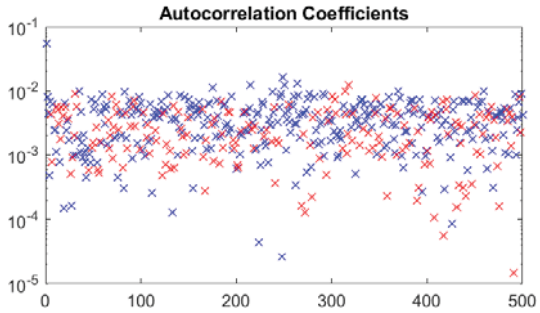

Fig. 3: Autocorrelation coefficients. Blue: positive. Red: negative.

by calculating the autocorrelation coefficients [13]. These coefficients are obtained by comparing the sequence with a delayed version of itself. They should be as low as possible and not follow any clear pattern. The results showed in Figure 3, for delays of up to 500 samples, exhibit values of autocorrelation below 10^{-2}. Positive (blue) and negative (red) values are fixed and no clear pattern can be found.

Then, the min-entropy [13]-[15] of the amplitude variations produced by the pulse collisions was estimated. This was done considering that this

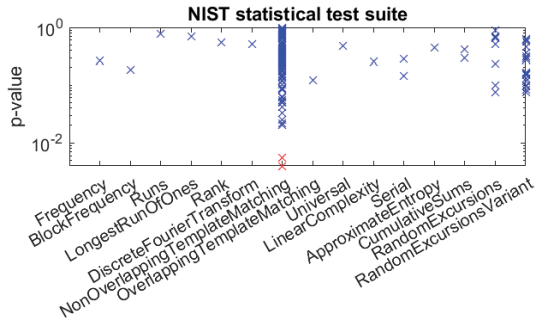

Fig. 4: P-values obtained on the NIST statistical test suite. Blue: >0.05. Red: <0.05.

effect is independent of the noise sources affecting the system. Under this assumption, the variance of the pulse collision can be obtained as the difference between the total variance and the variance of the noise. It also has to be taken into account the number of bits used for the digitalization, 16 in this case. The calculations resulted on an entropy estimation of 11.25 bits.

With the estimated value of the min-entropy, the entropy extraction process was done on the binary converted sequence. This is a technique by which a sequence of low entropy following a generic distribution, in our case gaussian, can be converted to a shorter sequence of higher entropy and homogeneous distribution. Among the different available techniques [16], the Toeplitz matrix, with a security factor ε of value 2^{-50}, was chosen.

The high entropy, homogeneous sequence obtained from the entropy extraction was then tested for its randomness with the NIST Statistical Test Suite [17], which are a battery of 15 tests that quantify the probability of a binary sequence to be random. The obtained results (Figure 4) show a high probability of the sequence being random.

Conclusions

We have designed, fabricated and characterized, in an InP standard platform, a fully integrated quantum random number generator based on phase fluctuations from a DBR laser diode, where all the optical components and photodiodes are integrated onto a single monolithic microchip. We showed that GHz rates of random numbers can be achieved with only 9mm^2 footpring and 118 mW total power consumption. The integrated laser source is an advantage in term of compactness and scalability and working with GS light simplifies the electronics design.

A logical future direction of this demonstration is to increase the random bit rate by means of a wavelengh multiplexing mechanism using GS laser tunability. Finally we expect our QRNG to find applications whenever a low impact, high rate source of random numbers will be required in integrated devices.

Acknowledgements

We wish to acknowledge H2020-MSCA-ITN-2018 EDIFY (Contract Number: 813467) and H2020 NEBULA project (Contract Number: 871658).

References

[1] B. Qi, Y.-M. Chi, H.-K. Lo, L. Qian, "High-speed quantum random number generation by measuring phase noise of a single-mode laser", Opt. Lett. 35, pp. 312–314, 2010.

[2] H. Guo, W. Tang, Y. Liu, W. Wei, "Truly Random Number Generation Based on Measurement of Phase Noise of Laser", Phys. Rev. E, vol. 81, N5 pp. 051137, 2010.

[3] F. Xu., B. Qi, X. Ma, H. Xu, H. Zheng, H.-K Lo, "Ultrafast quantum random number generation based on quantum phase fluctuations" Opt. Express 20, pp 12366-12377, 2012.

[4] C. Abellan, V. Pruneri, "The future of cybersecurity is quantum", IEEE Spectrum 55, vol. 5, pp 30–35, 2018.

[5] C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauerer, U. L. Andersen, C. Marquardt, G Leuchs,"A generator for unique quantum random numbers based on vacuum state",. Nat. Photonics 4, pp 711–715, 2010.

[6] T. Symul, S.M. Assad, P.K. Lam, P.K., "Real time demonstration of high bitrate quantum random number generation with coherent laser light", Appl. Phys. Lett. 98, pp 231103, 2011.

[7] X. Li, A.B. Cohen, T.E. Murphy, R. Roy, "Scalable parallel physical random number generator based on a

superluminescent LED", Opt. Lett. 36, pp 1020–1022, 2011.

[8] M.Herrero-Collantes, J. C. Garcia-Escartin, "Quantum random number generators", Rev. Mod. Phys. 89, 015004, 2017.

[9] F. Raffaelli et. al., "Generation of random numbers by measuring phase fluctuations from a laser diode with a silicon-on-insulator chip," Opt. Express 26, pp 19730-19741, 2018.

[10] M. Rudé et. al., "Interferometric photodetection in silicon photonics for phase diffusion quantum entropy sources," Opt. Express 26, pp 31957-31964, 2018.

[11] C. Abellán et. al., "Quantum entropy source on an InP photonic integrated circuit for random number generation," Optica 3, pp 989-994, 2016.

[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, pp 20665-20672, 2011.

[13] 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, vol. 20, no. 11, p. 12366, May 2012.

[14] B. Qi, "True randomness from an incoherent source," Rev. Sci. Instrum., vol. 88, no. 11, p. 113101, Nov. 2017.

[15] Bruen, A.A., Forcinito, M., 2005. Cryptography, information theory, and error-correction: a handbook for the 21st century. Wiley-Interscience, Hoboken, N.J.

[16] 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, vol. 87, no. 6, Jun. 2013.

[17] I. T. L. Computer Security Division, "NIST SP 800-22: Documentation and Software - Random Bit Generation | CSRC," CSRC | NIST, 24-May-2016. [Online]. Available: https://csrc.nist.gov/projects/random-bit-generation/documentation-and-software. [Accessed: 12-Feb-2019].