Quantum Random Number Generator based on Phase Diffusion in Lasers using an On-chip Tunable SOI Unbalanced Mach-Zehnder Interferometer (uMZI)

Muhammad Imran[1], Vito Sorianello[2], Francesco Fresi[2], Luca Potì[2], Marco Romagnoli[2]
[1]TeCIP Institute, Scuola Superiore Santanna Via Moruzzi 1, 56124 Pisa Italy,
[2]CNIT,Via Moruzzi 1, 56124 Pisa Italy,
muhammad.imran@santannapisa.it.

Abstract: A 12.5Gb/s QRNG based on phase diffusion in gain switched lasers is demonstrated using a packaged on-chip SOI tunable unbalanced MZI achieving minimum entropy/bit of 5.04 for 8 bit sample passing all NIST randomness tests.

1. Introduction

Random numbers play a crucial role in diverse applications such as secure communications, stochastic modelling, Monte Carlo simulations and extensive data processing. Quantum random number generators (QRNG) are a subset of physical random number generators that derive randomness from quantum mechanical processes [1]. Optical QRNG implementations have been investigated using different quantum processes as entropy sources including photon arrival time, amplified spontaneous emission, detection of vacuum field and phase noise in laser diodes [2]. However, most of these demonstrations use bulk, fiber or free space components which have large size, high cost and exhibit long term instability. Significant reduction in size is essential for integration into complex systems such as quantum key distribution receiver. Similarly larger size and higher cost reduce scalability and limit widespread commercial use. Instability issues strongly affect the reliability of these devices. To achieve low cost scalable solutions there has been a huge interest in photonic integrated circuits (PIC) technologies for quantum optics recently. A number of on-chip QRNG solutions for well investigated schemes have been reported in literature demonstrating different levels of complexities and integration (full/partial) using different integration technologies [3-5]. Silicon photonics has the advantage of direct integration with CMOS electronics hence increasing its deployment prospects in advanced semiconductor industry. Raffaelli et al. [3] demonstrated optical integration of a homodyne detector on a silicon-on-insulator (SOI) chip for 1.2 Gb/s QRNG based on vacuum fluctuations. Authors in [4] recently demonstrated SOI integrated QRNG based on phase fluctuations from an off-chip laser diode, all other components were integrated on SOI chip. Rude et al. demonstrated interferometric photo detection on a Si chip using an integrated unbalanced Mach-Zehnder interferometer (uMZI) scheme for a quantum entropy source based on accelerated phase diffusion [5]. The input MMI coupler of uMZI were designed to provide unbalanced splitting ratio (2% and 98%) and 1*ns* delay line. Differently from [5], in this work we demonstrate an alternative scheme for uMZI shown in Fig. 1 that uses an additional MZI in upper arm for tunable loss balancing between uMZI arms hence providing tunable control on maintaining high interference quality. The waveguides in 400 ps delay line are specifically designed for reduced loss. A shorter delay helps to achieve relatively higher data rates and improves resilience to temperature variations. Tunable power balancing and mid-way monitoring port can help to improve the long term stability of the QRNG through feedback control. NIST recommendation SP800-90B [6] suggests mechanisms for health tests of entropy sources therefore spare mid-way and output ports in proposed uMZI design can provide probes for health tests. The designed uMZI is fabricated on SOI platform and packaged providing electrical and fiber connectivity and thermal control. A QRNG is demonstrated using a phase diffusion quantum entropy source based on gain switching (GS) in off-chip laser and packaged on-chip SOI tunable uMZI. The entropy source provides phase randomized pulses and uMZI translates phase fluctuations in successive pulses into amplitude fluctuations to generate raw random data. Raw data is post processed for entropy estimation and subsequent randomness extraction using Toeplitz hashing. The extracted data successfully passed all NIST randomness tests [7] and achieved random number generation rate of 12.5 Gb/s.

2. Integrated Tunable Interferometer Design and Packaging

As depicted in Fig. 1, the PIC design consists of an uMZI having a 400ps delay line in the bottom arm and an additional balanced MZI equipped with thermo-optic phase modulators (TOPM) in the top arm. The MZI in the top arm is used to balance the extra loss experienced in delay line of the bottom arm by applying DC voltage to TOPMs in MZI and achieve DC loss balancing condition. The second output of the branch MZI (port 4 in Fig. 1) can be used as mid-way monitor for the quality of the input pulses and loss balancing. The input MMI coupler equally splits the input signal (pulses) with 50/50 splitting ratio. The pulses in the two arms experience different delay and temporal

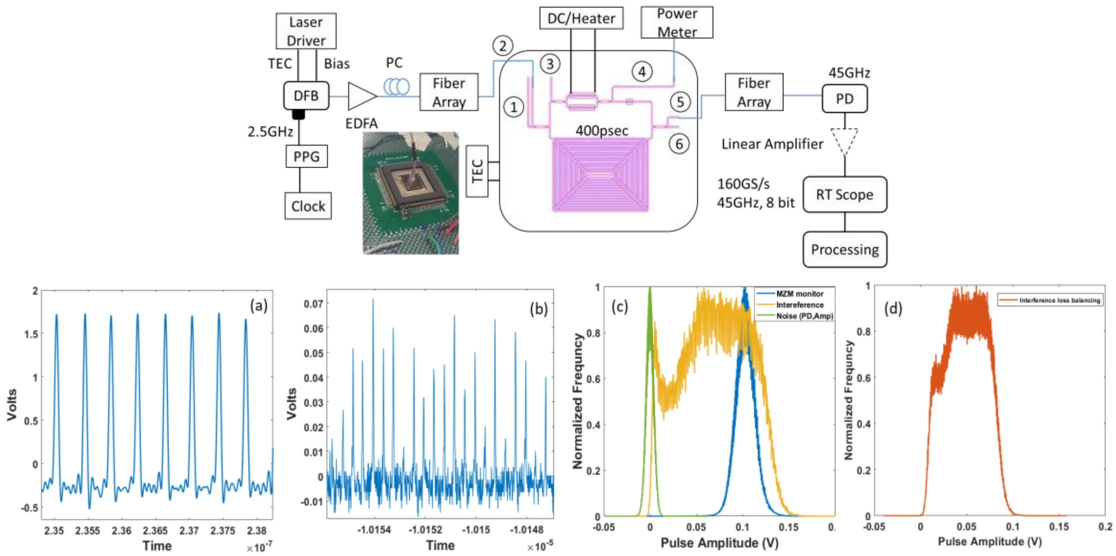

Fig. 1 (top) Experimental setup for QRNG based on phase diffusion in gain switched lasers and interference in on-chip SOI uMZI (a) phase randomized nearly equal amplitude pulses from GS laser (b) Pulses at uMZI output after interference (c) Histogram of noise, input and interference signal (d) Histogram of interference signal with loss balancing.

overlap between successive pulses i.e., interference is achieved at the output MMI by matching delay with input pulses repetition rate (400 ps corresponding to 2.5 GHz). The PIC is realized by e-beam lithography on a standard SOI platform with 220 nm thick Si overlayer and 3 µm thick buried oxide (BOX). We used single mode waveguides 480 nm wide with average propagation loss of 2.5 dB/cm and group index ng=4.2. In order to reduce the propagation loss of the delay line and the consequent insertion loss of the PIC, we designed the delay line with wider waveguides. The lower propagation loss is because of a reduced interaction of the fundamental mode field with the sidewalls of the waveguides, the main factor for the scattering loss. We designed a rectangular spiral where the straight sections are made of 1.5 µm wide waveguides (ng=3.6), while bends are realized with 480 nm wide waveguides in order to avoid excitation of high order within the bends. Adiabatic tapers are used between wider and narrow waveguide to ensure higher order modes are not excited. The spiral for 400 ps delay line has 50 turns (8µm internal radius), the gap between adjacent waveguides is 3.98µm, with an overall footprint of 370 µm x 490 µm and effective length of 3.33 cm. The overall loss is expected to decrease to 7.36 dB. This loss is balanced with the MZI in the top arm to improve the interference quality at the output of the uMZI. The PIC size is 7.5 mm x 7.5 mm (actual footprint of scheme on PIC is 2.61 mm x 5.77 mm including optical and electrical connections) and is housed in a 160LD Quad package on a thermoelectric cooling Peltier. The PIC temperature is monitored via negative temperature coefficient thermistor attached to it. The integrated device is wire bonded with the package to provide DC connections for heaters, thermistor and TEC. The whole package is attached to a custom made printed circuit board (PCB) for external DC connectivity. A 12 fiber array provides interface between on-chip and off-chip optical devices. The fiber array is glued to the chip and aligned to an 8 grating coupler (GC) array with 8° coupling angle and has a 12 port MPO connector for off-chip connections. The coupling loss for each GC was measured ~ 4.5 dB (10 dB for loop, loop length 0.21cm x 2.5 dB/cm= 0.53 dB).

3. Experiment and Results

The experimental setup is depicted in Fig. 1. A 1550 nm, 10 GHz DFB laser (Gooch & Housego AAA0701) is directly modulated by a train of narrow electrical pulses at 2.5 GHz generated by pulse pattern generator (Anritsu MP1800A). The peak of the electrical pulse excites gain in semiconductor medium and valleys bring laser below threshold causing attenuation. Resultantly optical pulses with nearly equal amplitude and random phase are produced. The threshold current I_{th} for DFB laser is 13 mA. Laser diode controller (ILX LDC-3900) provides the bias current and temperature control (25.67 °C) for DFB laser. To ensure phase randomized pulses at the output of the laser in GS mode we bias laser much below the threshold I_{DC} and setting RF driving signal at V_{pp}=1.5V i.e., I_{pp}= 23.8 mA (50 Ω termination). The laser output is amplified by erbium doped fiber amplifier (EDFA) coupled to a packaged on-chip uMZI via fiber array. A polarization controller is included between EDFA and PIC package to adjust the input polarization in order to reduce the coupling losses due to input GC on the chip. The optical interference signal at the output of the uMZI (port 5 in Fig. 1) is coupled to an external high bandwidth (45 GHz, 0.7 A/W) photo-detector (PD). The photocurrent from PD is further amplified through a highly linear 40 GHz linear electrical amplifier and converted to voltage signal. The continuous voltage signal is sampled and digitized using a

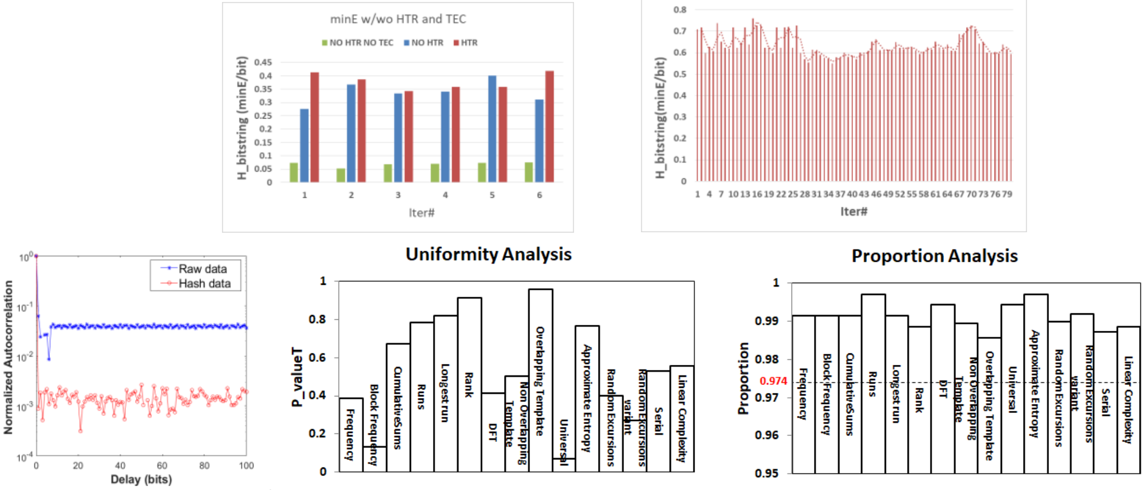

Fig. 2 Post processing: (top left) minimum entropy/bit with and without applying TEC control and loss balancing i.e., heaters in TOPMs. (top right) Estimated min. entropy per bit for 80 1M sample iterations using NIST SP-80090B entropy assessment tool, average min Ent/bit 0.63 (8*0.63= 5.04) (bottom left) Normalized autocorrelation coefficients for raw and hashed data (bottom centre and right) NIST Randomness evaluation results for 350 1Mbit hashed sequences: To pass a test P-value should be > significance level α=0.01 and to pass uniformity analysis Pvalue_T≥ 0.0001 (i.e., P-value of P-values). To pass proportion analysis, proportion of sequences satisfying (P>α) should be more than 0.974.

real time oscilloscope (Keysight DSO-Z 634A 160 GS/s, 45 GHz, 8bit). The scope is synchronized with a synchronization signal from PPG to accurately sample the interference signal. The pulses at the input and output of uMZI after are shown in the Fig. 1 (a, b). We also recorded histograms of electrical noise (green), mid-way monitoring signal (blue) which is effectively an attenuated input signal and output interference signal (orange) for nearly 500k samples (events) as shown in Fig. 1(c) for statistical verification of the expected behavior of the setup. The power distribution of the noise depicts the overall noise of the system mainly coming from photodiode and electrical amplifier. Broadening of output signal power can be clearly seen due to interference of phase randomized pulses as expected. We also recorded histograms after balancing the signal levels in the two arms of uMZI to improve the interference quality as shown in Fig. 1(d). Raw data was acquired from scope in three operating conditions (1) No TEC, No loss balancing (2) TEC, No Loss Balancing (3) TEC, Loss balancing of PIC. The acquired data were then post-processed offline as detailed below.

4. Post processing: Estimation of minimum entropy, randomness extraction and statistical testing

We estimated the minimum entropy both by using analytic formulas for this scheme and NIST entropy assessment tool in order to quantify randomness for the raw data. As evident from results in Fig. 2 (top right) entropy is maximized in the presence of TEC control and loss balancing through heaters. We acquired 80x1M samples in optimum condition and evaluated min entropy per bit for each iteration that was found to be on average approximately 5. The random data was extracted from raw data by applying Toeplitz Hashing randomness extraction algorithm using reduction factor RF= 5/8. It is clear form Fig. 2 (bottom right) that the hashed data has lower normalized autocorrelation compared to raw data. 350 1M bit hashed sequences were tested and successfully passed both uniformity and proportion analysis tests of NIST randomness tests as shown in Fig. 2.

5. Conclusions

A QRNG providing random data rate of 12.5 Gb/s is demonstrated using on-chip tunable packaged SOI uMZI that provides improved interference quality, tunability and input/output monitoring for feedback control.

Acknowledgement: The PIC was fabricated by INPHOTEC and work was supported by ENYGMA project.

References

[1] Miguel Herrero-Collantes and Juan Carlos Garcia-Escartin, “Quantum random number generators”, Rev. Mod. Phys. 89, 015004 (2017)
[2] Xiongfeng Ma et al. “Quantum random number generation”, npj Quantum Information volume 2, 16021 (2016)
[3] F. Raffaelli et al. “A homodyne detector integrated onto a photonic chip for measuring quantum states and generating random numbers,” Quantum Sci. Technol. 3, 025003 (2018).
[4] Francesco Raffaelli et al. "Generation of random numbers by measuring phase fluctuations from a laser diode with a silicon-on-insulator chip," Opt. Express 26, 19730-19741 (2018).
[5] M. Rudé et al."Interferometric photodetection in silicon photonics for phase diffusion quantum entropy sources,"Opt. Exp 26, 31957-64(2018)
[6] K. McKay and J. Kelsey, GitHub -usnistgov/SP800-90B EntropyAssessment, https://github.com/usnistgov/SP800-90B_EntropyAssessment.
[7] A. Rukhin et al. “A statistical test suite for random and pseudorandom number generators for cryptographic applications,” NIST Special Publication 800-22 revision 1a (2010).