Photonic integration of quantum entropy sources

(Invited paper)

C. Abellan[1*], W. Amaya[1], M. Rudé, D. Tulli[1], M. W. Mitchell[2,3] and V. Pruneri[2,3]
[1]Quside Technologies S.L., C/Esteve Terradas 1, 08860 Castelldefels (Barcelona), Spain
[2]ICFO-The Institute of Photonic Sciences, The Barcelona Institute of Science and Technology, 08860 Castelldefels (Barcelona), Spain
[3]ICREA-Institució Catalana de Recerca i Estudis Avançats, Lluis Companys 23, 08010 Barcelona, Spain

ABSTRACT

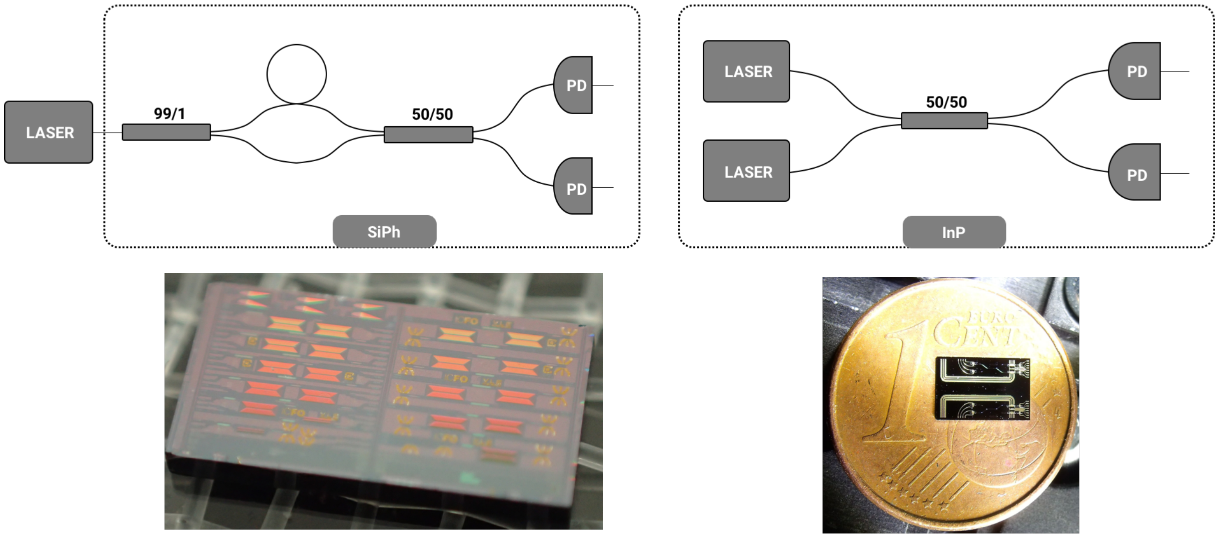
In this talk, we will discuss recent progress on the miniaturisation of ultrafast quantum entropy sources based on the phase-diffusion mechanism present in pulsed semiconductor lasers. Recent results of the integration in silicon photonics and indium phosphide platforms will be presented, demonstrating that Gb/s quantum random number generation is feasible with current photonic integration technologies. This shows potential towards mass scale adoption of quantum and photonic components for cyber-security and super-computation.

Keywords: quantum technologies, integrated photonics, quantum entropy sources.

1. INTRODUCTION

Random number generators play a crucial role in many information technologies, such as cryptography, numerical simulations in engineering, science or finance, and gambling. Historically, multiple techniques have been used to produce random bits, including algorithmic processes, known as pseudo-random number generators. However, only through the detection of quantum mechanical dynamics one can generate truly unpredictable random numbers. Various quantum random number generators (QRNGs) have been proposed during the last 30 years, mostly based on photonic approaches. Some examples include single photons splitting, the measurement of arrival time of single photons or the detection of vacuum fluctuations using homodyne measurements. To date, schemes based on the phase diffusion (PD) process in semiconductor lasers have achieved the fastest bit rates (up to tens of Gb/s) [1]. Randomness metrology procedures have been applied to PD-QRNGs to make quantitative statements about the unpredictability of this type of devices [2], and multiple prototypes have been built to be used in stringent environments, such as in the case of the 2015 loophole-free Bell test experiments [3]. Discrete optical components and optical fibres have been mostly utilised so far, posing limitations to the integration levels that can be achieved, and thus limiting the applicability of the technology to niche markets only. Remarkably, recent progress in the photonic industry can now be exploited to build compact and cost-effective devices with the potential to extend the market reach of quantum random number generators. Here, we present recent results towards the miniaturisation of phase diffusion quantum entropy sources (PD-QES) using Silicon Photonics [4] and Indium Phosphide [5] platforms.

The PD-QESs described in this manuscript are based on the phase diffusion process present in pulsed semiconductor lasers. By pulsing a laser from well below to well above its threshold level, a stream of phase-randomised optical pulses, with nearly identical intensity profiles, is generated [1-3]. When the laser is in its on state, stimulated emission dominates and coherence is created inside of the cavity. However, during the off-time, large phase diffusion is experienced and full randomisation occurs. This macroscopic phase diffusion process is a result of spontaneous emission events occurring inside of the laser cavity, and has therefore a quantum mechanical nature. After a string of phase-random pulses is created, an interferometric setup can be used to convert this now macroscopic phase information into the amplitude domain. In this way, one can obtain a stream of macroscopic amplitude-random pulses. This signal can be detected with standard high-bandwidth telecommunications photodetectors and digitised using commercial analog-to-digital converters. A quantum random number generator is therefore a device that produces random bits starting from a quantum mechanical process, or more precisely, a device that produces random numbers after taking samples directly from a quantum entropy source component.



A) SiPh chip based on an uMZI layout

B) InP chip based on a two-laser layout

Fig. 1. Integrated phase diffusion quantum entropy sources. (A) Silicon Photonics layout and chip based on an unbalanced Mach-Zehnder interfererence scheme. (B) All-optical integration in Indium Phosphide using a novel two-laser interference scheme.

2. PHOTONIC INTEGRATION

Two material platforms dominate the design and development of advanced photonic integrated circuits to date: Silicon Photonics (SiPh) and Indium Phosphide (InP). The key driving force behind SiPh is the ability to use CMOS like fabrication resulting in high-volume production at low cost. Besides CMOS compatibility, SiPh also offers high levels of integration. However, SiPh does not count with an easy integration of a laser source, limiting therefore the scope of the functionalities that can be pursued with this material platform. Alternatively, InP offers efficient integration of laser sources, opening the door to a whole new range of applications that can be monolithically integrated. In this section, we describe the development of two integrated quantum entropy sources in the two main integrated photonic platforms.

In Fig. 1A), the SiPh integration of a PD-QES based on an unbalanced Mach-Zehnder interferometer (uMZI) is shown [4]. In this configuration, the long path of the uMZI delays the pulse train by one period with respect to the short path, effectively achieving the interference of subsequent optical pulses at the output of the interferometer. The chip was designed to operate at 1 GHz frequencies, thus requiring a delay line of ~7 cm. At the output of the interferometer, fast germanium photodiodes are integrated on-chip to detect the interfered signal. An external 10 GHz gain-switched DFB laser was used as a light source to generate the input string of phase-randomised optical pulses. The uMZI is built with two cascaded multimode interferometers (MMIs) and a spiral delay line. Due to the relatively long 7-cm delay line, a ~20 dB loss is incurred by the signal travelling the long path of the uMZI, causing a significant loss unbalance between the two arms of the Mach-Zehnder . To compensate for such a loss unbalance, a 99/1 MMI was used at the input of the MMI to pre-compensate the loss incurred in the long path. Thus, the signal travelling the short path experiences a ~20 dB loss after the first MMI compared to the signal in the long arm, which will accumulate the ~20 dBs when travelling the spiral structure. Finally, when both signals reach the second 50/50 MMI, they both accumulate a 20 dB loss, thus optimising the interference visibility. The interfered signal is detected by the integrated photodetectors, demonstrating the functionality of the chip at an operating frequency of 1 GHz. The SiPh die area is below 1mm x 0.5mm. Future steps include the integration of the laser source on-chip using hybrid or heterogeneous techniques.

In Fig. 1B), the integration of a PD-QES on InP is depicted. In this case, and with the objective to reduce the losses introduced by long delay lines, a new design based on a two-laser scheme is introduced [5]. In this InP chip, all the photonic components are monolithically integrated on the chip, thus achieving full optical integration of the quantum device. In this new heterodyne detection configuration, one of the two lasers is operated in gain-switching mode to produce a string of phase-random pulses, whereas the other is operated in continuous wave (CW) mode and acts as a local oscillator. The output from the two lasers is combined at a 50/50 MMI. By tuning the central frequency using metallic contacts on the laser structures, and by bringing the frequency detuning within the detection bandwidth of the integrated photodetectors, the random beat note between the GS and the CW lasers can be detected. The integrated device is tested for time intervals of up to 12-hours, finding high operation and statistical stability. The full optical integration in InP is achieved in a die size below 6mm x 2mm. In contrast to the uMZI layout described in the SiPh chip, the two-laser scheme can be operated at an arbitrary frequency, thus enabling full speed tunability. The chip has been tested at 200 MHz due to digitisation limitations, but pulsing rates above the GHz regime have been successfully observed, thus enabling multi-Gb/s entropy production in a fully integrated chip.

3. CONCLUSIONS

We have demonstrated the integration of phase-diffusion quantum entropy sources using standard chip production processes in Indium Phosphide and Silicon Photonics. Bit-rates above Gb/s have been obtained in both cases, showing progress towards mass-scalable ultrafast quantum entropy sources. These devices can be used to generate high-speed and high-quality unpredictable bits, which are of fundamental importance in cryptography, super-computation and gambling applications.

REFERENCES

[1] C. Abellan, W. Amaya, M. Jofre, M. Curty, A. Acin, J. Capmany, V. Pruneri, and M. W. Mitchell, “Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode”, Optics express **22**, 2, 1645–1654 (2014)

[2] M. W. Mitchell et al., “Strong experimental guarantees in ultrafast quantum random number generation”, Phys. Rev. A **91**, 012314 (2015)

[3] 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)

[4] M. Rudé, C. Abellan, A. Capdevila, D. Domenech, M.W. Mitchell, W. Amaya and V. Pruneri, “Phase diffusion quantum entropy source on a silicon chip”, arXiv:1804.04482v1 (2018)

[5] Abellan, C., W. Amaya, D. Domenech, P. Muñoz, J. Capmany, S. Longhi, M. Mitchell, and V. Pruneri: “Quantum entropy source on an InP photonic integrated circuit for random number generation”, Optica **3** (9), 989–994 (2016)