Design of a fully integrated quantum number generator

V. Moskalenko[1], R. Broeke[1], E. Bente[2], D. A. Outerelo[3], P. Vilar-Gomez[3], F. J. Diaz Otero[3]

[1]Bright Photonics, Horsten 1, 5612 AR Eindhoven, The Netherlands
[2]Eindhoven University of Technology, 5600 MB Eindhoven, The Netherlands
[3]University of Vigo, EI Telecomunicacion, 36310 Vigo, Spain

Random numbers are an essential resource for different applications such as secure communications, numerical simulation or quantitative finance. Quantum random number generators (QRNGs) based on phase diffusion have achieved high bit rates and passed severe random tests, making this method adequate to obtain random numbers [1]. However, so far, they have been realized with discrete optical components, often leading to devices of large size and high power consumption. In this work we demonstrate the design of a monolithically integrated QRNG. The photonic integrated circuit (PIC) was designed for InP technology available through Smart Photonics multi-project wafer runs. The schematic of the QRNG is shown in Figure 1 (a). In this configuration a Gain-switched (GS) laser produces periodic pulses, which propagate through two Mach-Zehnder interferometers (MZIs) in series. An integrated photodetector (PD) at the end of the circuit converts the light into an electrical signal. The MZI 1 balances the power of the input to the arms of the MZI 2 for maximal extinction ratio, while MZI 2 converts random phase variations between the consecutive optical pulses into amplitude variations, which the PD detects.
Despite the availability of the required components in integrated platforms, the PICs are less flexible than their bulk prototypes. This means that a lot of attention should be paid to the component specification in the design stage of the PIC, in particular that of the laser source. It is important that the GS laser provides single mode operation and the laser reaches a quantum noise level between pulses. The first condition is necessary for efficient interference between the pulses in MZI 2, whereas the second condition is required in order to obtain phase randomness between the pulses. In addition, the laser should operate at relatively high speeds (up to 1 GHz) and it should not require high RF input power. There are several ways to achieve single mode operating lasers in InP active-passive technology. In this work we have chosen to use a Fabry-Perot cavity with distributed Bragg reflectors (DBR) as mirrors. The laser performance was simulated using FreeTWM. The simulations show that single mode-performance can be achieved with right and a left DBRs having a relative shift in their reflection peak wavelength of approximately 1 nm. Figure 1 (b) shows the evolution of the optical spectrum of the DBR laser with spectrally shifted DBRs. Moreover, it was shown that depending on the spectral position of the laser emission with respect to the gain peak, a higher net gain modulation can be achieved at the same RF power. In other words, the laser exhibits a higher net gain variation when operating around the gain peak. Figure 1 (c) shows a time trace of the GS laser. The design of the rest of the circuit takes into account fabrication limitations, optical loss and extinction ratio constraints in the MZIs.

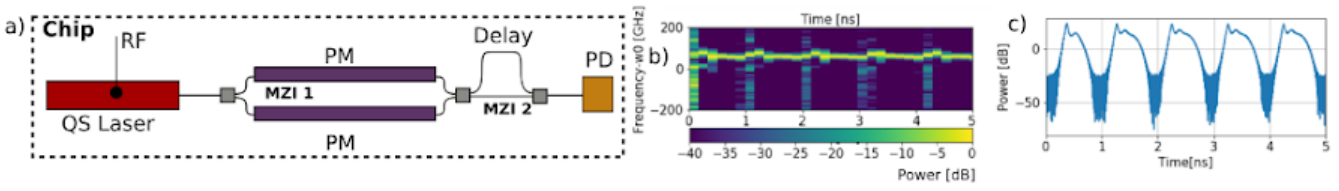

Figure 1: a) Sketch of the integrated QRNG. b) Simulated optical spectrum of the GS laser change in time . c) Simulated GS laser time trace.

In summary, we have proposed a design of the first fully integrated QRNG based on phase diffusion for realization in a generic monolithic photonic integration process. We have theoretically investigated laser performance and optimized the laser design for use in a QRNG circuit.

References

[1] M. Jofre, M. Curty, F. Steinlechner, G. Anzolin, J. P. Torres, M. W. Mitchell and V. Pruneri, “True random numbers from amplified quantum vacuum”, Optics Express, vol. 19, No. 21 (2011).