Versatile Random Numbers Extraction by Single Photon Detection

Andrea Stanco*[1], Davide G. Marangon[1], Giuseppe Vallone[1], and Paolo Villoresi[1]

[1]*Department of Information Engineering, University of Padova, Italy*

True randomness is achievable only by sampling a quantum physical process thanks to the intrinsically probabilistic nature of quantum mechanics. Quantum Random Number Generators (QRNGs) are fundamental in many fields of science and information technology. In particular, they can also be used in foundation Quantum Mechanics experiments[1, 2] which require timed-random number in order to close the *freedom of choice* loophole. Timed-random number means a number *created* after *trigger* t_A and before *deadline* t_B.

Our QRNG consists of a light source attenuated to single photon level and of one or more single photon detectors (SPDs) as well as a Field Programmable Gated Array (FPGA) board. The light source and the SPD generate and detect single photons while the FPGA is responsible for the generation and synchronization of the random bit in a specific time-window.

Several different generation protocols are implemented within the device and one can choose a protocol over the others depending on the specific application requirements. Protocols have different performances and are based on photons relative time of arrival, overall photon detection in time interval and randomness extraction algorithm[3, 4, 5]; they guarantee true randomness. A schematic example of one of these protocol is shown in figure 1.

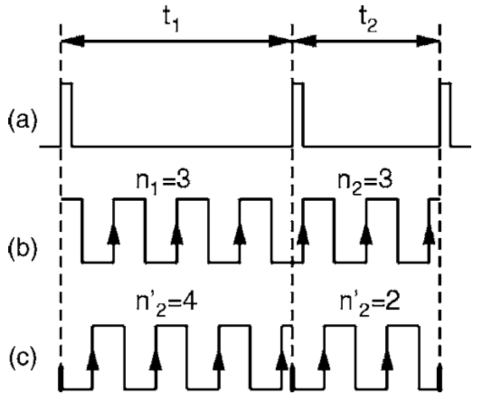

Figure 1: Comparing the number of events within a time-window defines whether is produced 0 or 1. Figure from [3].

Our QRNG takes advantage of the FPGA technology in order to yield random numbers with specific time requirements. As a matter of fact, this technology allows a perfect control over the time evolution of the QRNG since every operation is multiple of the fundamental time unit defined by the system clock. This feature guarantees a real-time behaviour and the synchronization of the device with an external trigger from an experiment. For a block schematic view see figure 2. Indeed, the device was successfully used in [1]. In addition to the quantum mechanics experiments, our device could be used in other fields including quantum communication, quantum and classical cryptography.

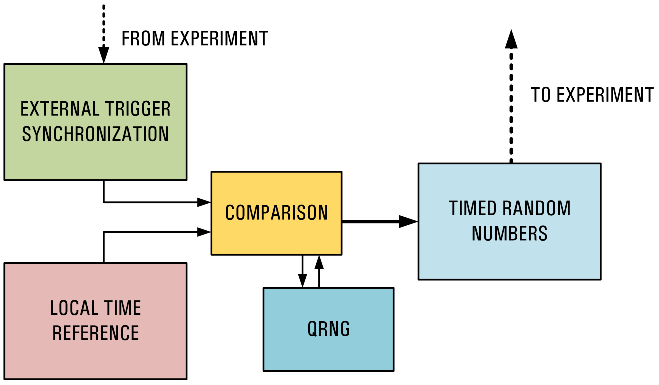

Figure 2: Block-schematic view of the time synchronization system between the QRNG and an external experiment.

References

[1] F. Vedovato et al., *Extending Wheeler's delayed-choice experiment to Space*, arXiv:1704.01911 [quant-ph] (2017).

[2] Carlos Abellan et al., *Generation of fresh and pure random numbers for loophole-free Bell tests*, Phys. Rev. Lett. **115**, 250403 (2015).

[3] M. Stipčević and B. Medved Rogina, *Quantum random number generator based on photonic emission in semiconductors*, Rev. Sci. Instrum. **78**, 045104 (2007).

[4] Martin Fürst et al., *High speed optical quantum random number generation*, Opt. Express **18**, 13029-13037 (2010).

[5] John von Neumann, *Various techniques used in connection with random digits*, National Bureau of Standards Applied Mathematics Series (1951), pp. 36–38.

*andrea.stanco@dei.unipd.it