Efficient quantum random number generation with full entropy extraction from SPAD based systems

Andrea Stanco [1,*], Davide G. Marangon [1,†], Giuseppe Vallone [1], Samuel Burri [2], Edoardo Charbon [2] and Paolo Villoresi [1]

[1] Dipartimento di Ingegneria dell'Informazione, Università degli Studi di Padova, Padova, Italy
[2] EPFL, Rue de la Maladiere 71b, 2002 Neuchatel, Switzerland
[†] Present address: Toshiba Europe Limited, Cambridge Research Laboratory, Cambridge, CB4 0GZ, UK

SUMMARY

Here we present a QRNG technique capable to extract all the available entropy from a randomness source and hence maximize the overall generation bitrate. We applied this technique to two different devices which integrate a Field Programmable Gate Array (FPGA): Randy, which includes one Single Photon Avalanche Diode (SPAD) and LinoSPAD, which includes a CMOS SPAD array as well as a Time-to-digital (TDC) converter.

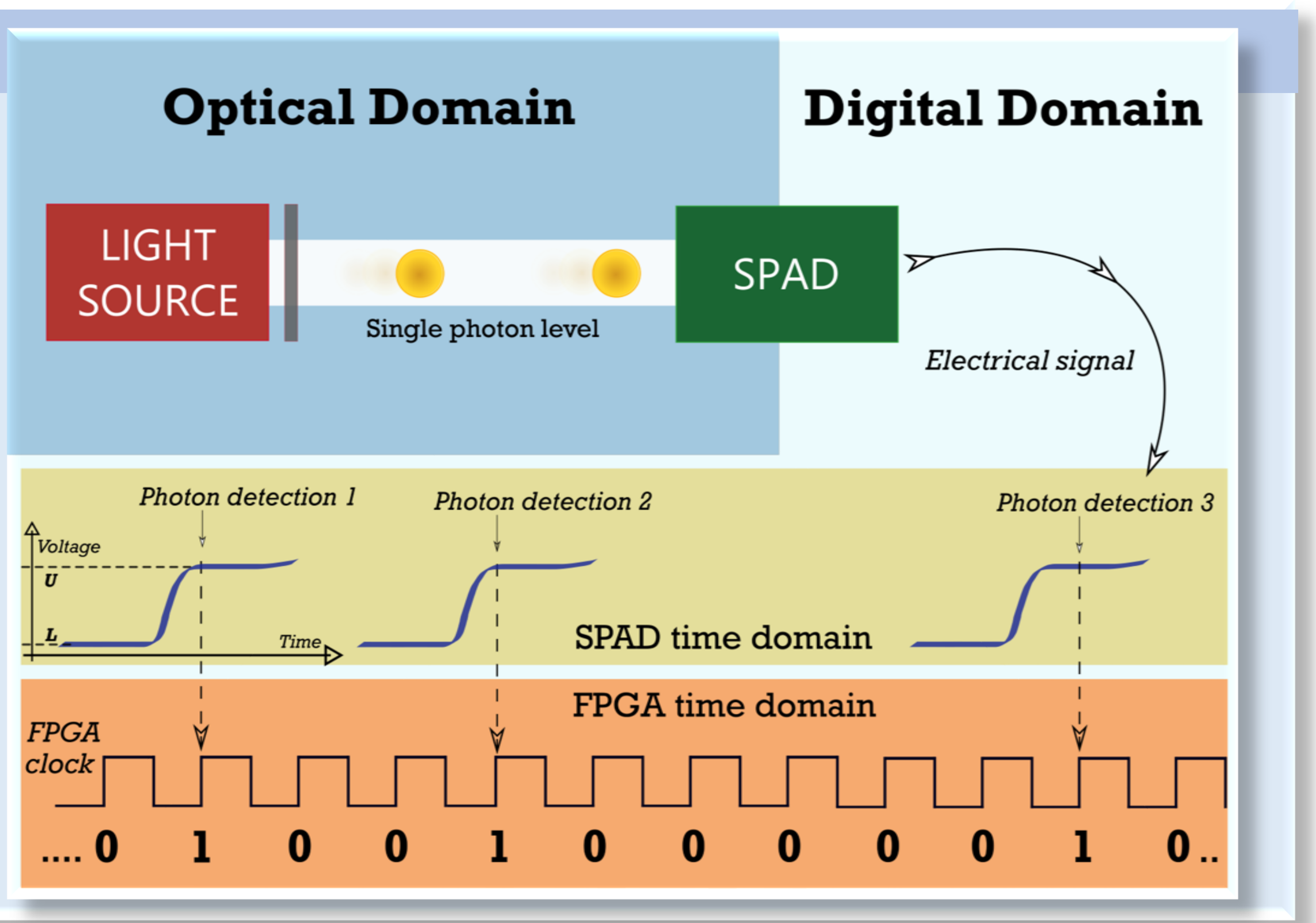
QRNG DEVICE

We realized a simple QRNG device that exploits the single photon time of arrival and a fast sampling clock signal [1]. With respect to other protocols that work with single photon time of arrival [2,3], our technique fully exploits all the potentiality of a given system.

A schematic view of the setup is visible in figure.

We attenuate a light source to single photon level and detect the photons with a Single Photon Avalanche Diode (SPAD) detector. The electrical signal output by the SPAD is sampled by a Field Programmable Gate Array (FPGA) board at a very high frequency with respect to the photon count rate (100 MHz vs. 200 kcount/s). The sampling process stores a '1' bit whenever an event occurs, otherwise it stores a '0' bit.

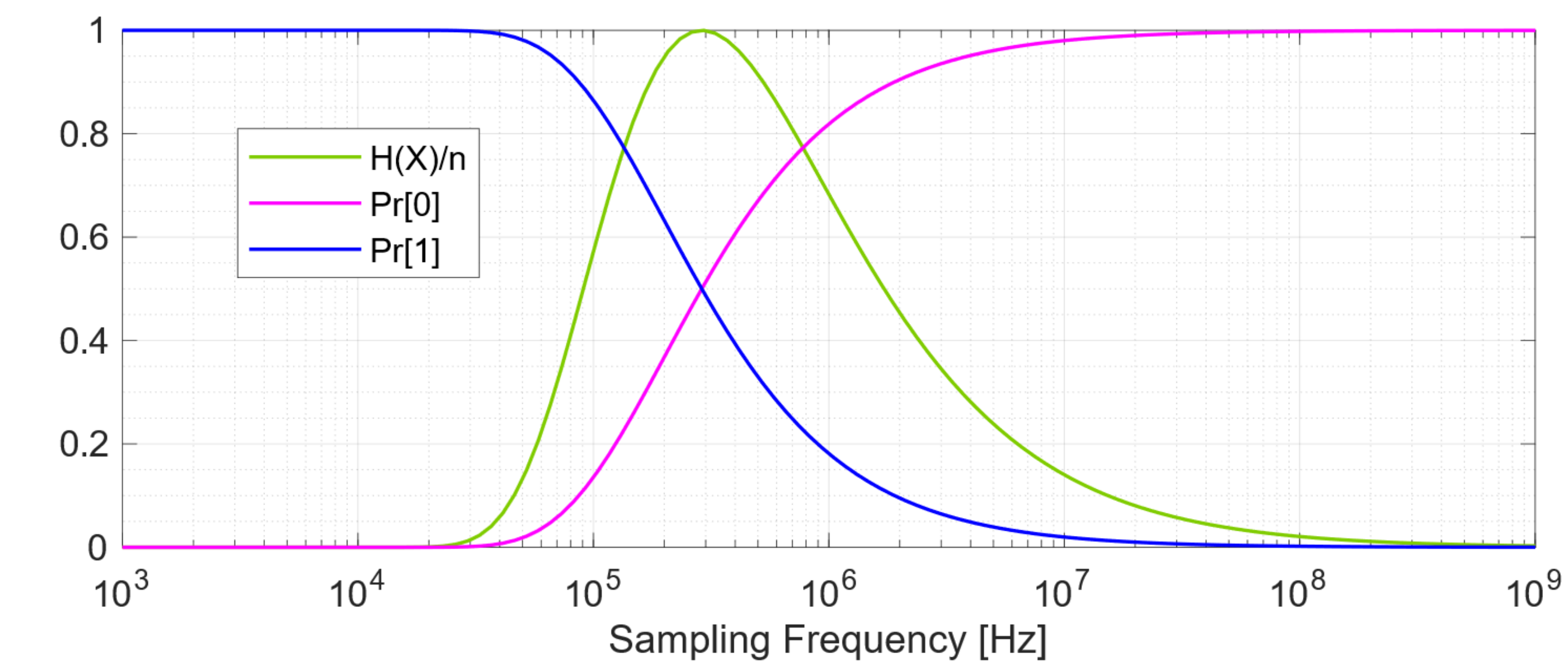
The key idea is to deliberately do an oversampling of the event stream and produce a heavily biased binary string because of the high unbalancing between sampling rate and photon count rate. Then, the SPAD non idealities (dead time and afterpulse) are removed and the Peres algorithm [4] is applied in order to remove the bias and have a true random data sequence.

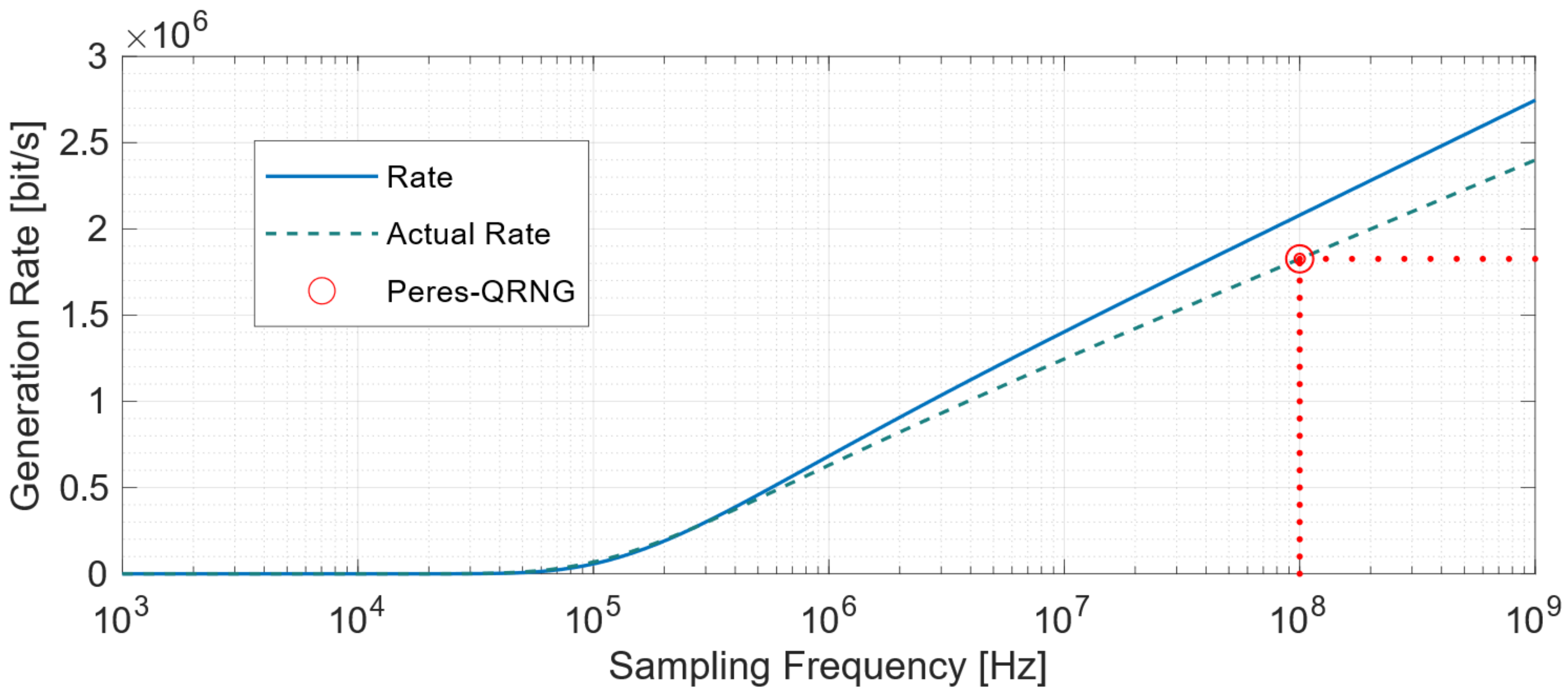


TECHNIQUE PRINCIPLE

According to the Poisson distribution formulas and to the expected Peres efficiency, it is possible to plot (figure below) the binary entropy and the Peres generation rate as function of the sampling rate (the photon count rate is fixed at 200 kcount/s).

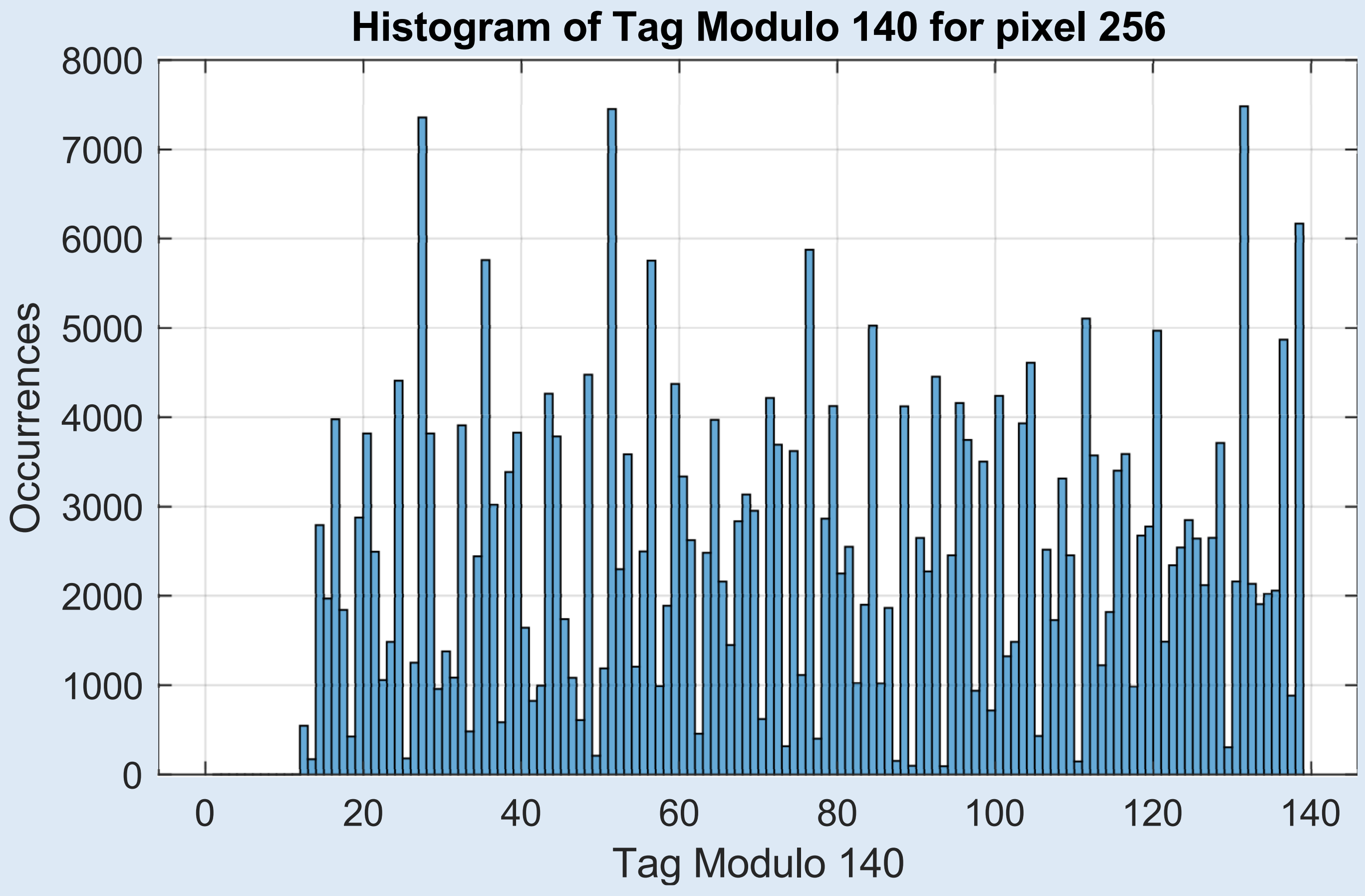
It is clear that having an unbiased system, i.e. binary entropy equal to 1, does not produce the highest bitrate. It is more convenient to oversample the signal, remove the SPAD non idealities and then apply Peres.





Figures, or slightly modified versions of, are taken from [1]

MULTIPLEXING THE GENERATION RATE



In order to improve the generation rate even more, we applied the same technique to a CMOS SPAD array device called LinoSPAD [5], a recent device from the AQUA lab at EPFL, which integrates 256 single photon detectors as well as 64 Time-to-Digital Converters (TDCs) with 17.9 ps resolution implemented on an FPGA. The generation stream was divided between **Coarse**, which belongs to the sampling clock, and **Fine**, which is related to the extra time resolution offered by the TDC. For the **Coarse** resolution we applied the same procedure of Randy. For the **Fine** one we had to deal with TDCs non idealities (figure below) and applied the Zhou-Bruck algorithm [6].

RESULTS

We tested a new technique to produce random numbers exploiting single photons time of arrivals. This technique maximize the generation bitrate for a given system and can also be applied to a multiple-SPAD system in order to improve the generation rate even more filling the gap with the CV-QRNG.

The final generation rates are:

❑ Single SPAD system, 200 kcount/s, 100 MHz sample rate = 1.8 Mbit/s
❑ LinoSPAD system, 1250 kcount/s, 400 MHz sample rate (+TDC) = 310 Mbit/s

REFERENCES

[1] A. Stanco et al., *Efficient random number generation techniques for CMOS single-photon avalanche diode array exploiting fast time tagging units*, Phys. Rev. Research 2, 023287 (2020).
[2] H. Fürst et al., *High speed optical quantum random number generation*, Opt. Express. (2010).
[3] M. Stipčević and B. M. Rogina, *Quantum random number generator based on photonic emission in semiconductors*, Review Of Scientific Instruments 78, 045104 (2007).
[4] Y. Peres, *Iterating von Neumann's procedure for extracting random bits*, Ann. Statist., vol. 20, pp. 590–597 (1992).
[5] S. Burri et al., *LinoSPAD: a time-resolved 256×1 CMOS SPAD line sensor system featuring 64 FPGA-based TDC channels running at up to 8.5 giga-events per second*, in Optical Sensing and Detection IV (SPIE, 2016).
[6] H. Zhou and J. Bruck, *A Universal Scheme for Transforming Binary Algorithms to Generate Random Bits from Loaded Dice*, arXiv:1209.0726 [cs.IT], (2012).

QuantumFuture
The shift in the communication paradigm
quantumfuture.dei.unipd.it
*andrea.stanco@unipd.it