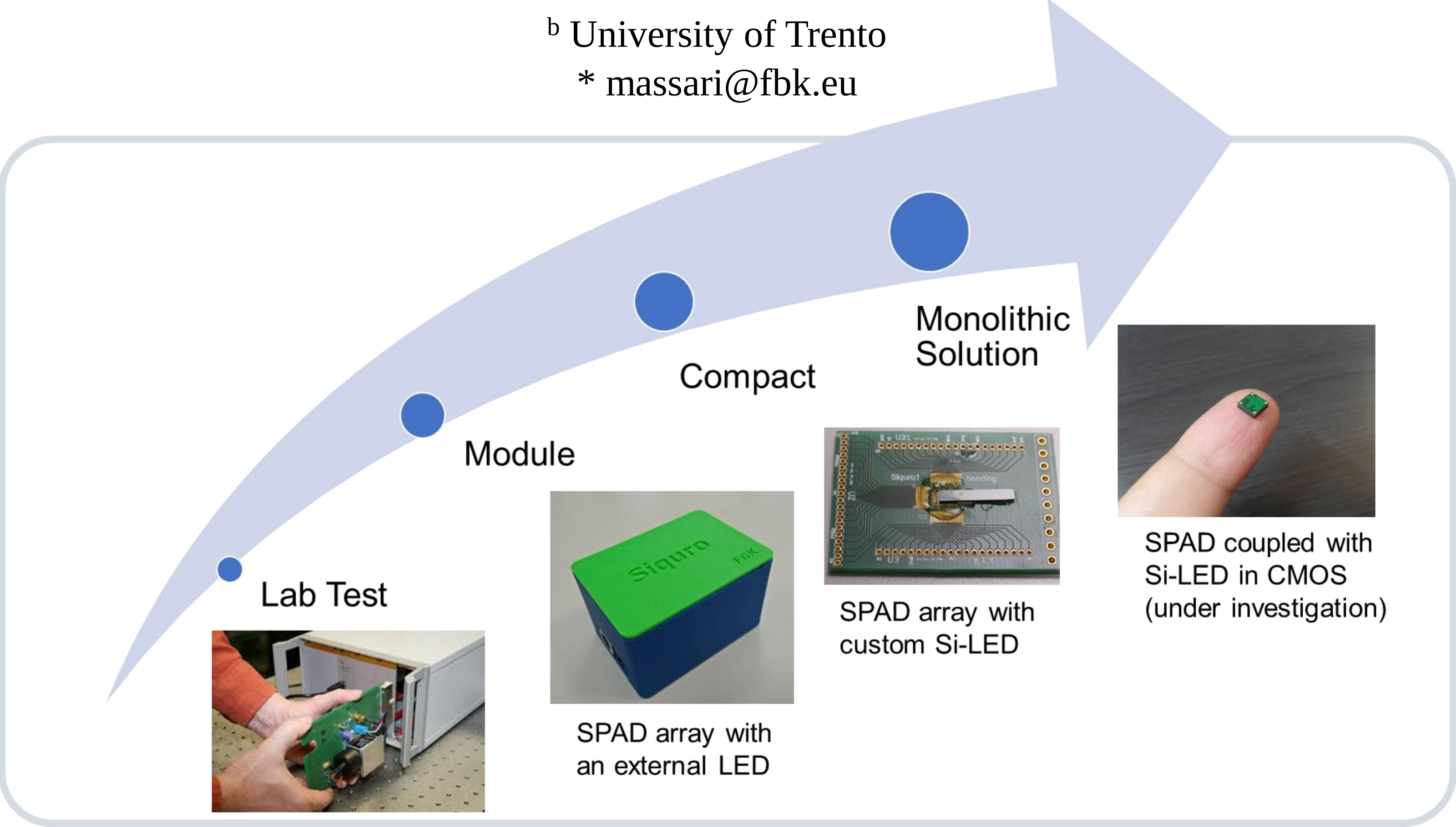
Compact Silicon Technology based Quantum Random Number Generators

Nicola Massari[a] *, Georg Pucker[a], Leonardo Gasparini[a], Nicola Zorzi[a], Fabio Acerbi[a], Matteo Perenzoni[a], Alessandro Tomasi[a], Zahra Bisadi[b], Enrico Moser[b], Giorgio Fontana[b], Alessio Meneghetti[b], Lorenzo Pavesi[b]

[a] Fondazione Bruno Kessler (FBK)

[b] University of Trento

* massari@fbk.eu



SPAD array with an external LED

SPAD array with custom Si-LED

SPAD coupled with Si-LED in CMOS (under investigation)

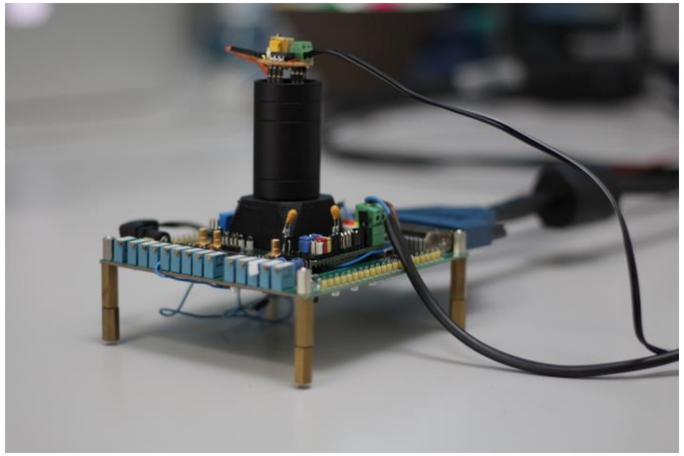
Introduction

Main issue of the IoT system is the need to establish a SECURE communication among devices of the network
We need to find a way to protect sensitive information from attacks

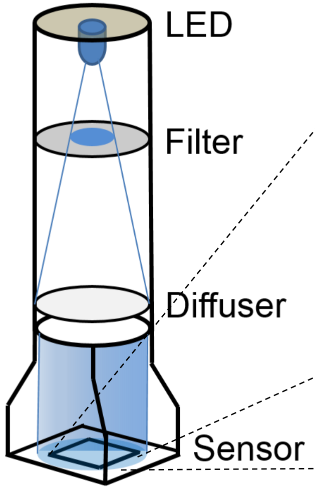
Internet of Things
30

QRNGs are fundamental buildings blocks for guaranteeing a secure communication, being able to produce secret keys for data encryption with high degree of unpredictability

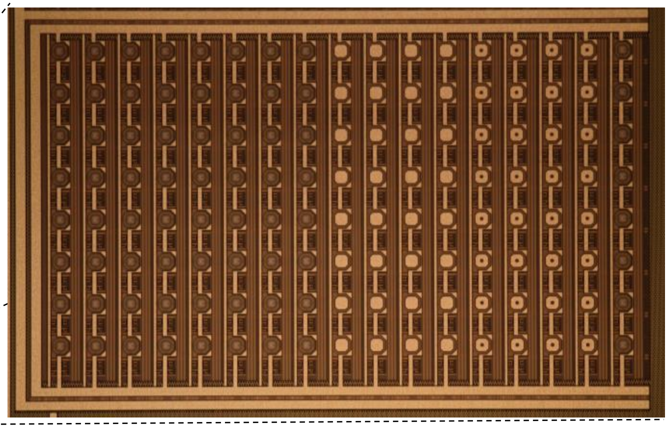
QRNG based on external LED



a. Test system



b. Optical setup

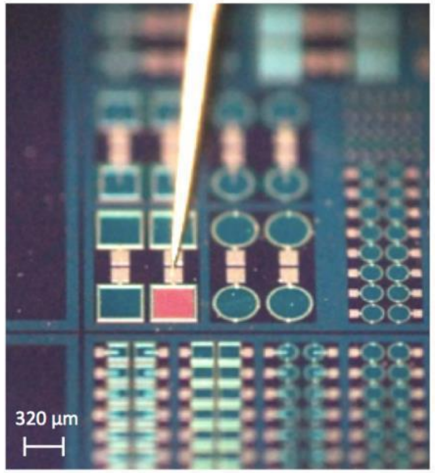


c. Array of SPADs

c. Final demo

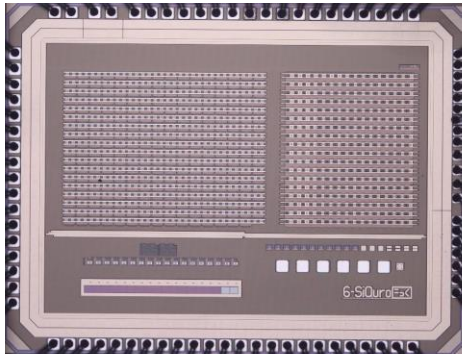
The system consists of an external LED properly attenuated and diffused, in order to uniformly illuminate a detector based on single photon avalanche diodes (SPAD). The detector is an array of 16x16 cells, each made by a couple of SPADs, working in parallel for increasing the bit rate generation. Each cell works as an independent QRNG and it generates random number starting from the measurement of the arrival time of photons

QRNG based on Si-nc-LED



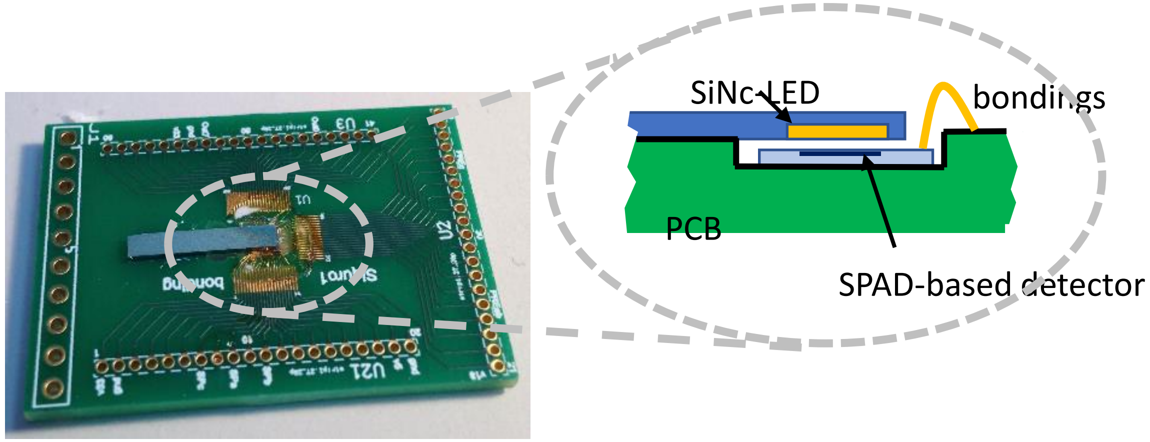
a. Si-nc-LED

+



b. CMOS SPAD array

=

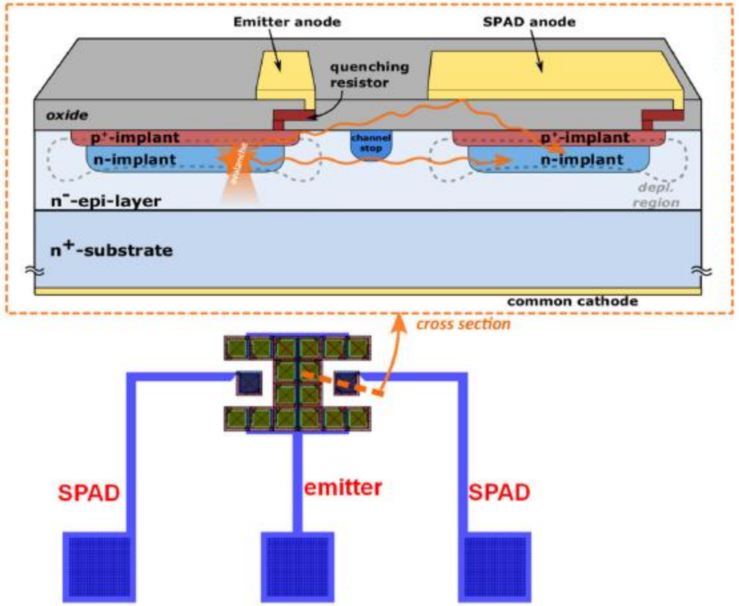


c. Assembled system

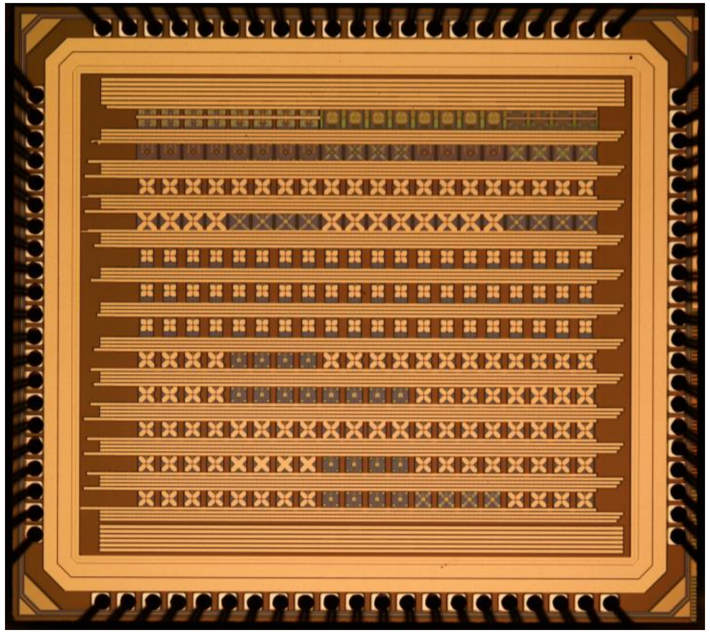
In order to increase the compactness of the QRNG, we combined two different technologies: a. the Silicon Nanocrystal LED (Si-nc-LED); c. standard CMOS SPAD array customized for the application. The final system shows a good compactness at the expense of a reduction of the generated bit rate (due to the low light intensity)

d. Demo

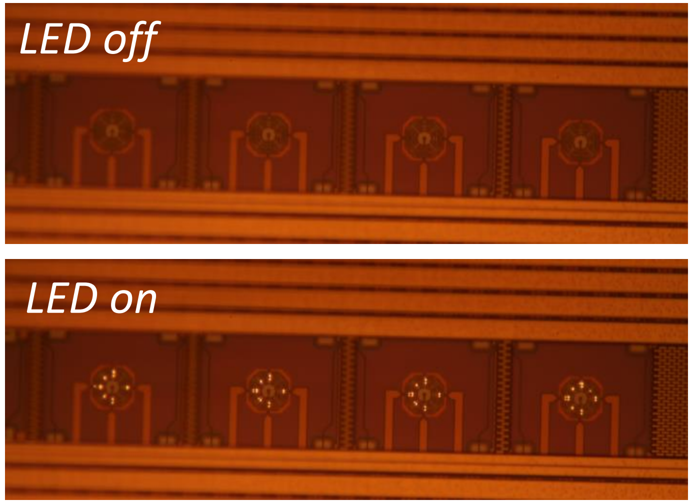
QRNG based on a monolithic approach



a. Monolithis QRNG based on custom process



b. Test chip using CMOS process



QRANGE

c. SiLED in CMOS

Implementation test structures proving the monolithic approach, where source of light and detection are implemented on the same substrate. We used two approaches: a.) we first demonstrate the principle using a custom process (FBK), then b.) we implemented test structures in a standard CMOS process.