# The path to a fully integrated Semi-Device independent QRNG

**N. Leone**[1], D. Rusca[2], S. Azzini[1], G. Fontana[1], F. Acerbi[3], A. Gola[3], A. Tontini[3], N. Massari[3], G. Fontana[1], H. Zbinden[2], and L. Pavesi[1]

1. Department of Physics University of Trento, Via Sommarive 14, Povo (TN), Italy
2. University of Geneve, 1205, Geneve, Switzerland
3. Fondazione Bruno Kessler, Via Sommarive 18, Trento (TN), Italy

UNIVERSITY OF TRENTO - Italy
DEPARTMENT OF PHYSICS
Nanoscience Laboratory

The generation of random numbers is an important requirement in many applications: one of the most important is information security, where these sequences are used to encrypt the transmitted information. Here, we present a fully integrated chip which is the building block of a quantum random number generator (QRNG) [1]. The chip (see figure 1) is based on a CMOS-compatible technology: both the sources of light and detectors are integrated in the same optical chip. The emitter is an array of independent SPADs, whereas the detector is a SPAD with a layout similar to the emitter cells. By using this device, we implement the Semi-Device independent protocol presented in [2], where the generation of the quantum random numbers is certified by an estimation of the minimum achievable entropy. This is also robust against manufacturing tolerances and performance variability of the detectors, increasing the overall quality and security of the generation itself, thanks to the self-testing nature of the protocol. The detailed description of the experiment is reported in [3].

## The silicon photonic chip [1]

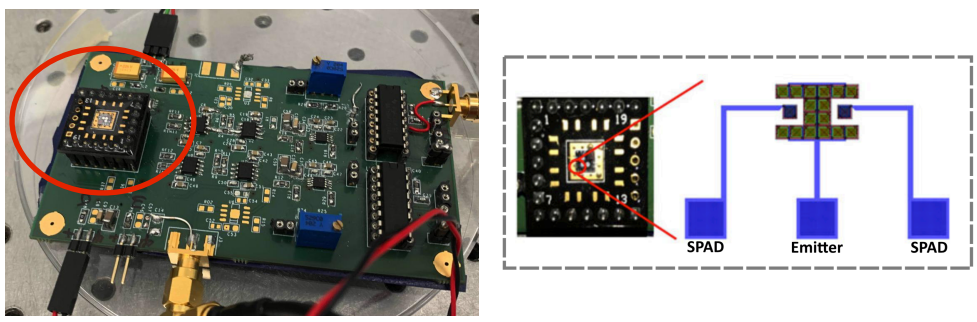


Figure 1: **Structure of the chip**. It is composed by 16 emitters, and 2 detectors.

## The semi-device independent protocol [2] : Prepare-and-measure setup.

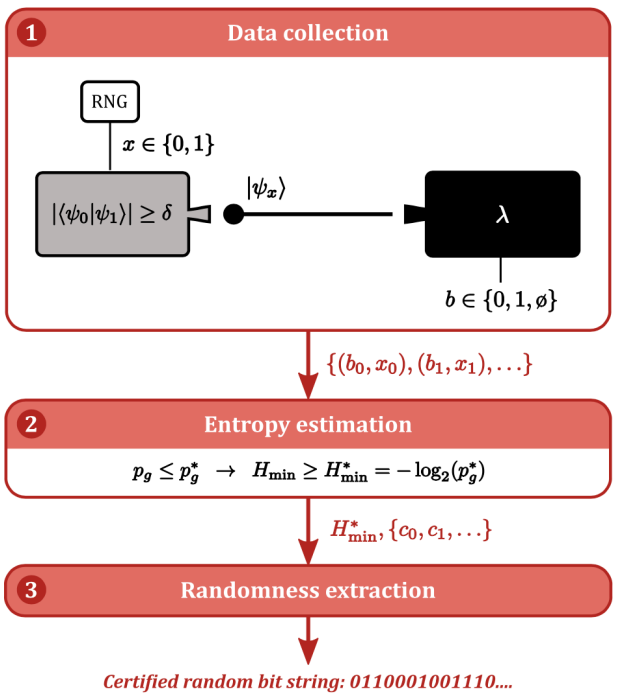


Figure 2: **QRNG protocol**.
The protocol is reported in [2].

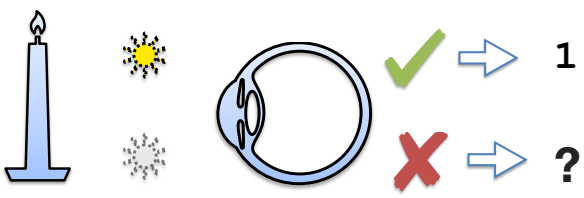


Figure 3: **Quantum nature of the process.** The detector cannot be sure if $|\alpha\rangle$ or $|0\rangle$ are coming since they are not orthogonal.

The detector is treated as a **black box,** and no assumption are performed over it.
A PSRNG fixes the input x that is feed to the emitter, that emits the state $|\alpha\rangle$ or $|0\rangle$ based on the outcome. The two states need to be non-orthogonal.
Knowing the overlap $\delta$, the conditional probabilities $\mathbb{P}(b/x)$ are calculated, and an estimation of the $H_{min}$ is given, by the use of the protocol.

$$|\alpha\rangle = e^{\frac{-|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle$$

$$\langle 0|\alpha\rangle = \delta = e^{\frac{-|\alpha|^2}{2}}$$

## Experimental results

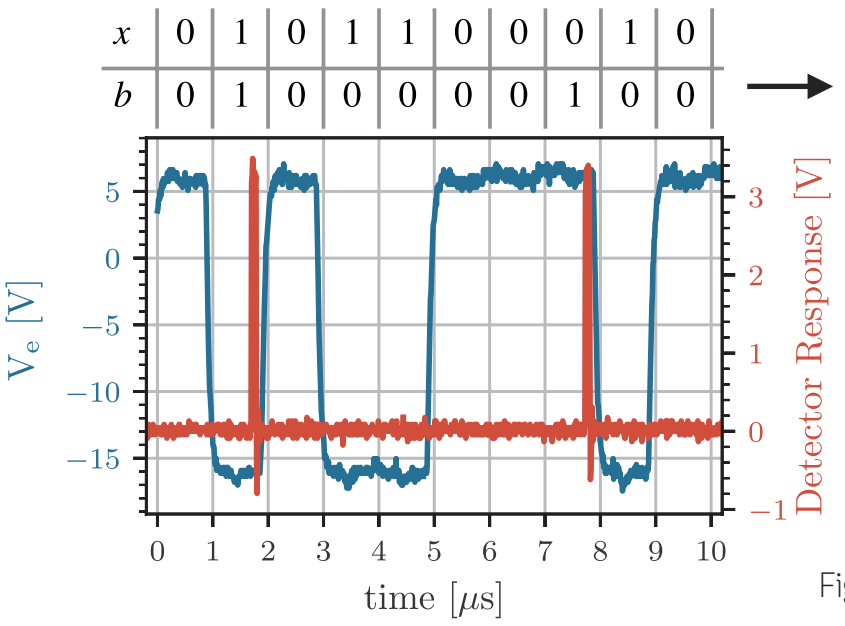


Figure 4: **Example of the acquisition data**. Based on the protocol reported in [2].

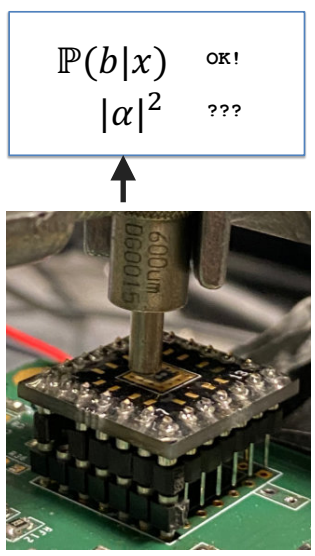


Figure 5: **Measure of the $\alpha$.** Measurement used to characterize the number of photons per pulse.

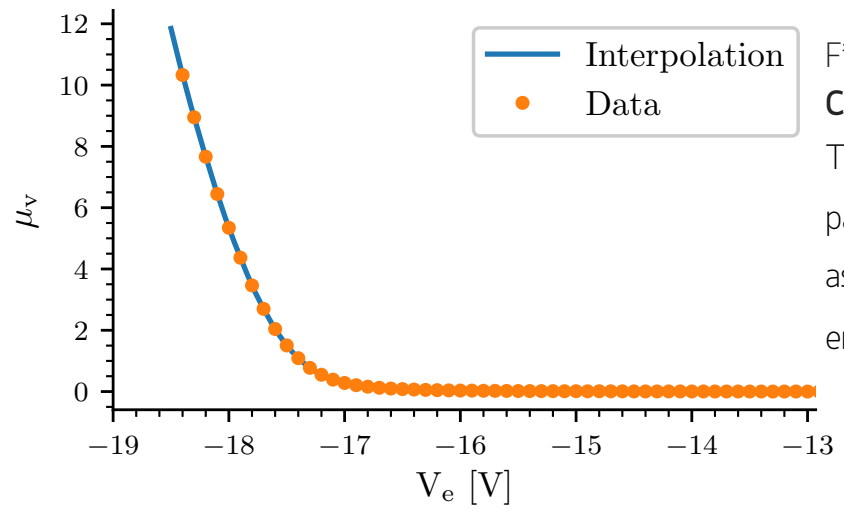


Figure 6: **Characterization curve.** The $|\alpha|^2 = \mu_v$ parameter is measured as a function of the emitter voltage $V_e$.

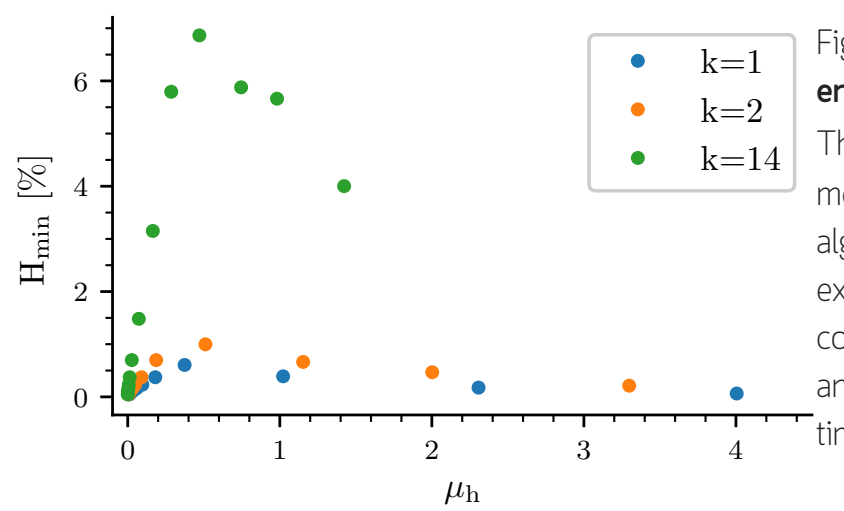


Figure 7: **Minimum entropy.** The $H_{min}$ parameter is measured using the algorithm of entropy extraction starting from conditional probabilities and the mean flux over a time window.

$H_{min} \simeq 0.6\,\%$ **@1MHz obtained in [3]**

[1] Fabio Acerbi, Zahra Bisadi, Giorgio Fontana, Nicola Zorzi, Claudio Piemonte, and Lorenzo Pavesi. A Robust Quantum Random Number Generator Based on an Integrated Emitter-Photodetector Structure. doi: 10.1109/ JSTQE.2018.2814787.

[2] Jonatan Bohr Brask, Anthony Martin, William Esposito, Raphael Houlmann, Joseph Bowles, Hugo Zbinden, and Nicolas Brunner. Megahertz-Rate Semi-Device-Independent Quantum Random Number Generators Based on Unambiguous State Discrimination. doi: 10.1103/PhysRevApplied.7.054018.

[3] Nicolò. Leone, Davide Rusca, Stefano Azzini, Giorgio Fontana, Fabio Acerbi, Alberto Gola, Alessandro Tontini, Nicola Massari, Giorgio Fontana, Hugo Zbinden, and Lorenzo Pavesi, An optical chip for self-testing quantum random number generation, https://doi.org/10.1063/5.0022526