Towards certified QRNG based on Single Particle Entanglement

N. Leone[1], S. Azzini[1], S. Mazzucchi[2], L. Pavesi[1]*

1 Nanoscience Laboratory, Department of Physics, University of Trento, Via Sommarive 14, Povo (TN), Italy
2 Department of Mathematics and TIFPA-INFN, University of Trento, Via Sommarive 14, Povo (TN), Italy
**nicolo.leone@unitn.it*

In this work we apply single-particle entanglement of photons to the generation of genuine random numbers. The certification of randomness is achieved through the measurements of the minimum entropy by the Bell's test.
Keywords: QRNG, Single-particle Entanglement

Abstract

Random numbers are fundamental tools to ensure information security. Their importance relies on the possibility of cipher information by the use of a starting random sequence, which is called "the key". Without knowing the latter, it is then impossible to access to the information. Consequently, the generation of a genuine random sequence results to be mandatory to ensure the secrecy of the communication. Nowadays, random numbers are mostly obtained by mathematical algorithms, where only the complexity of the mechanism is the assurance of security. This is dangerous, since an algorithm is a deterministic process and its results can be predicted. Other methods of generation are based on chaotic properties like thermal fluctuations or noise in a device. In this case, the certification whether the process itself is random is not possible since the complication of the mechanism hinders its deterministic behaviour. Consequently, chaotic sources do not rule out the possibility for an adversary to predict the sequence based on a better knowledge of the underlying mechanism.

In this scenario Quantum Physics, in particular quantum optics, offers a unique possibility: thank to the probabilistic nature of the quantum description of nature it is possible not only to have random outcomes of a measurement, but also to certify the randomness of the source.

Following the work of S. Pironio et al. [1], here we present a proof-of-concept application of single-particle entanglement (SPE) [2] to the quantum generation of random numbers (QRNG). SPE is a peculiar type of entanglement in which two degrees of freedom (DoFs) of the same particle are entangled: in our experiment we use photons. By an attenuated laser beam we entangle the momentum and polarization DoFs of single photons in a set-up based on off-the-shelf linear optical components, like polarizers and beam splitter. Single Photon Avalanche Detectors (SPAD) detect the photons and generate raw sequences of random numbers by the different outcomes obtained in the measurements.

In particular, we probe the violation of the Bell's inequality in the CHSH form [3], which ensures SPE and gives an a-priori certification of the intrinsic randomness of our random numbers. In addition, the violation of the inequality yields an estimation of the minimum entropy of the outcomes [1]. Having access to this information is crucial, since it allows to transform, with the use of postprocessing techniques [4], the raw numbers obtained in the experiment, into a real sequence of unbiased random numbers. This ensures that our sequence is unpredictable by any classical theory.

Compared to traditional inter-particle entanglement, where photons are generated by nonlinear processes which require high power lasers, SPE can be obtained by attenuated laser with only linear optical components like beam-splitters and polarization rotators.

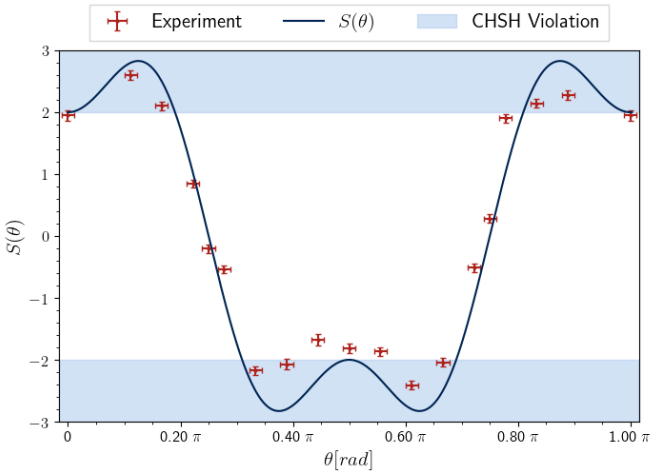

Fig. 1: Violation of the Bell Inequality as a function of the parameter θ, the angle that controls the polarization. The red points are the experimental data, while the solid curve is the theoretical behaviour of the CHSH correlation function S. The cyan zone represents the region where the violation of the CHSH inequality occurs.

Acknowledgements

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 820405 project QRANGE, and by the India-Trento Programme of Advanced Research ITPAR phase IV project. The work of N.L. was supported by a Q@TN grant.

References

1. Pironio, S., Acín, A., Massar, S. et al. *Nature* **464,** 1021–1024 (2010).
2. Gadway, B. R., Galvez, E. J. & De Zela, F. *J. Phys. B: At. Mol. Opt. Phys.* **42** 015503 (2009).
3. Clauser, J. F., Horne, M. A., Shimony, A. et al. *Phys. Rev. Lett.* 23, 880–884 (1969).
4. Nisam, N. & Ta-Shma, A. *J. Comput. Syst. Sci.* 58, 148-173 (1999).