Ultrafast and passive source-device-independent Quantum Random Number Generator

M. Avesani,[1] D.G. Marangon,[1] G. Vallone,[1] and P. Villoresi[1]

[1] *Department of Information Engineering, University of Padova, 35131 Padova, Italy*

ABSTRACT

Random numbers play a vital role in many areas such as lotteries, scientific simulations, cryptography and fundamental physics tests.

In this work, we propose a novel method based on the sampling of continuous-variable quantum systems for the generation of secure random numbers, suitable for cryptographic applications, at ultrafast rates.

The setup implements a double optical homodyne detection for the simultaneous measurement of the quadratures of an incoming quantum state, typically the vacuum. This method improves the approach described in[1] because removes the need of an active switch and at the same time increases the generation rate.

The analysis of the extractable true quantum randomness is performed in a paranoid scenario where an eavesdropper can control the source (source-device-independent). Also in such unfavorable case, ie, with the eavesdropper preparing the quantum states, we are able to estimate a lower bound to the extractable entropy, even in presence of classical or quantum side-information held by the eavesdropper. By employing fast balanced detectors for the measurement of the quadratures our system is capable of generating more than 11 Gbps of certified random numbers.

---

[1] D. G. Marangon, G. Vallone, and P. Villoresi, Physical Review Letters **118**, 060503 (2017).