Entropy source evaluation of a vacuum fluctuation based quantum random number generator

Arne Kordts[1*], Cosmo Lupo[2], Dino S. Nikolic[1], Thomas B. Pedersen [3], Tobias Gehring[1], Ulrik L. Andersen[1]

1. Technical University of Denmark (DTU), Kgs-Lyngby, Denmark
2. University of York, York, United Kingdom
3. Cryptomathic A/S, Aarhus C, Denmark

[*] *arnek@fysik.dtu.dk*

Quantum random number generators [1] (QRNGs) offer genuine randomness for cryptographic solutions with unconditional security based on our current understanding of nature alone. The security of each QRNG implementation is based on the strength of assumptions, which have to be made about the used measurement protocol. The most rigorous and secure approach hereby are so called device-independent protocols [2], based on Bell-test like measurements, but these are still limited to low generation rates. By including assumptions about device performance higher generation rates can be achieved. So far, the performance of such devices was most commonly verified by running a battery of statistical tests, like those used for the evaluation of deterministic software-based pseudo random number generators (PRNG), on the generated output. The security of these device-dependent implementations depend on an accurate discrimination between the classical and quantum contribution of a recorded signal [3], as it was done for phase-diffusion QRNG [4].

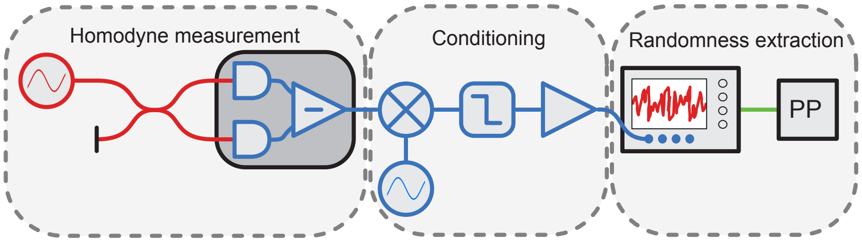

Fig. 1. Vacuum fluctuation QRNG scheme. A shot-noise limited homodyne detection of the vacuum is performed. Part of the detector output is selected by down-mixing and conditioning the signal onto the analog to-digital converter range. Random extraction is performed by post-processing (PP) the raw-data using Toeplitz-hashing.

Here we present such an accurate assessment for an entropy source of a vacuum fluctuation based QRNG setup [5], see Figure 1. The strength of this approach lies in the fact that the vacuum is intrinsically pure. By characterizing all device components we perform an effective quantitative measurement of the vacuum fluctuation power spectral density equal to $\hbar\omega$. Further, in previous implementations the classical noise contribution, introduced by the device components, were assumed to be uncorrelated, here we characterize and consider these in the conservative estimation of the minimal extractable entropy. Random number extraction was implemented on a FPGA board using Toeplitz-hashing. The current work contributes towards a security evaluation standard of high generation-rate device-dependent QRNG implementations.

References

1. Herrero-Collantes, M., Garcia-Escartin, J. C. (2017). Quantum random number generators. Reviews of Modern Physics, 89(1), 15004.
2. Acin, A., Masanes, L. (2016). Certified randomness in quantum physics. Nature, 540(7632), 213219.
3. Hart, J. D., Terashima, Y., Uchida, A., Murphy, T. E., Roy, R. (2016). Commentary: Evaluating photonic random number generators. http://arxiv.org/abs/1612.04415
4. Mitchell, M. W., Abellan, C., Amaya, W. (2015). Strong experimental guarantees in ultrafast quantum random number generation. Physical Review A - Atomic, Molecular, and Optical Physics, 91(1), 110.
5. Gabriel, C., Wittmann, C., Sych, D., Dong, R., Mauerer, W., Andersen, U. L., Marquardt, C., Leuchs, Gerd Leuchs, G. (2010). A generator for unique quantum random numbers based on vacuum states. Nature Photonics, 4(10), 711715.