The impact of digitization on the entropy generation rates of physical sources of randomness

Joseph D. Hart[1], Thomas E. Murphy, and Rajarshi Roy

Institute for Research in Electronics and Applied Physics,
University of Maryland, College Park
[1]email address: jhart12@umd.edu

Random number generation underlies the modern cryptographic techniques used to ensure the privacy of digital communication and storage. In order to improve security, digital information systems increasingly utilize physical entropy sources to add unpredictability to traditional deterministic pseudo-random algorithms. Traditionally, statistical tests applied to random bit generators have considered only the final post-processed bit sequence, which obscures the physical origin and limitations of the original entropy source. The new NIST draft standards described in SP 800-90B begin to address these issues by placing an emphasis on understanding the physical principles governing the entropy source and determining the rate of entropy generation directly from the raw data. However, the importance of digitization—a key process common to all physical random number generation techniques—has thus far received little attention in the evaluation of physical entropy sources.

We highlight the importance of the interplay between the physical origin of the entropy and the digitization of the entropy source on the limits of entropy generation. Our study of the entropy generation rates of three state-of-the-art optical entropy sources demonstrates the importance of understanding the dependence of the entropy generation rates on the resolution of both the observable and of time. We estimate the entropy generation rates using both the min-entropy tests recommended by NIST SP 800-90B as well as an estimate of the information entropy [1] and [2], and find qualitatively similar results: the physical origin of the entropy depends crucially on the resolution of the digitization process.

Reference:

1. Cohen, A., and I. Procaccia, "Computing the Kolmogorov entropy from time signals of dissipative and conservative dynamical systems." *Phys. Rev. A* **31.3** (1985): 1872.
2. Hagerstrom, A.M., T.E. Murphy, and Rajarshi Roy, “Harvesting entropy and quantifying the transition from noise to chaos in a photon-counting feedback loop”, *Proceedings of the National Academy of Sciences* **112.30** (2015): 9258-9263.