Scilight

NEWS | AUGUST 21 2017

Using the Cohen-Procaccia function to extract entropy origin in photonic random number generators FREE

Rachele Hendricks-Sturrup

Scilight 2017, 090009 (2017)
https://doi.org/10.1063/1.5000832

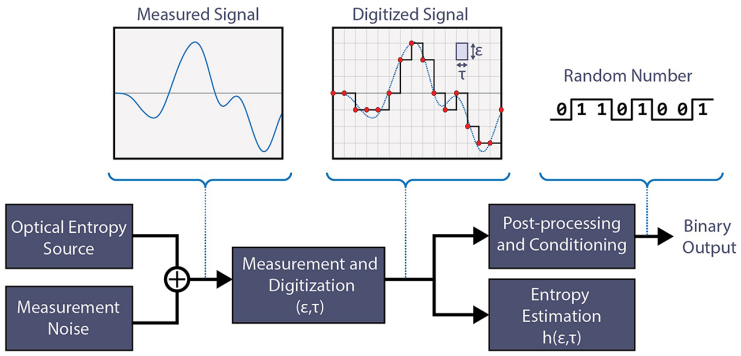
Scilight

25 August 2017

Using the Cohen-Procaccia function to extract entropy origin in photonic random number generators

Rachele Hendricks-Sturrup

Researchers use cutting-edge algorithm to uncover the physical origin of entropy and its effect for photonic random number generators.



Traditional random number generators (RNGs) currently lack accurate methods of measuring true randomness, or entropy, that would ensure the protection of private information from hackers. To address this gap, researchers at the University of Maryland and Laboratory for Telecommunication Sciences in Maryland and Saitama University in Japan present in *APL Photonics* the Cohen-Procaccia rate analysis validation method of quantifying entropy generation and optical limitations in RNGs.

The Cohen-Procaccia algorithm contains a function of the time-tagging measurement resolution ε and sampling period τ, or h (ε, τ), separating stochastic and chaotic entropy sources during the RNG evaluation process to measure the relationship between ε and τ and uncover the physical origin of entropy. Therefore, the authors assess the Cohen-Procaccia entropy estimate in a physical RNG with a single photon time-of-arrival detection source and further compare the Cohen-Procaccia entropy estimates against the most common value (MCV) and the Markov estimates in the physical RNG with chaotic lasers and amplified spontaneous emission entropy sources.

In the single photon time-of-arrival detection source, using photon rates 2.3 Mcps and 5.37 Mcps, the authors found that the Cohen-Procaccia entropy rate estimate agreed well with their approximated function of photon time-of-arrival. For the chaotic laser source, the Cohen-Procaccia algorithm interestingly exposed an insufficient, yet correctable, level of randomness in MCV and Markov estimates at high sampling rates. They obtained similar results for the ASE source; the Markov and Cohen-Procaccia estimates perform similarly when $N = 3$, but not when $N \geq 7$.

Moving forward, in their paper, the authors recommend that RNG designers converge their raw RNG entropy analysis data against the Cohen-Procaccia estimate to quantify true randomness and ensure an appropriate sampling rate.

Source: "Recommendations and illustrations for the evaluation of photonic random number generators," by Joseph D. Hart, Yuta Terashima, Atsushi Uchida, Gerald B. Baumgartner, Thomas E. Murphy, and Rajarshi Roy, *APL Photonics* (2017). The article can be accessed at https://doi.org/10.1063/1.5000056.