Limitations of using the coherent sampling method for random number generation

Gauthier Achard Baccati[1,2]

[1] CEA-Leti, Grenoble, France

[2] LabHC, Saint-Etienne, France

Abstract

Many true random number generators (TRNGs) rely on ring oscillators (ROs) and their inherent jitter as a source of randomness. Entropy can be determined using various techniques, such as coherent sampling. This work investigates a phenomenon observed in coherent sampling ring oscillator TRNGs that arises when the sampling period is of the same order of magnitude as the jitter. Under these conditions, irregularities in the sampling process can result in truncated values - either in terms of bits or counter values - which we hereby refer to as "glitches". We analyze this behavior in two configurations: (1) a COSO-TRNG implemented as an application-specific integrated circuit (ASIC), and (2) a Python-based emulator. Notably, the emulator exhibits a significantly higher incidence of glitches, which we attribute to the absence of metastability filtering by flip-flops. To address this, we propose a method for handling glitches which preserves key TRNG performance metrics, including entropy and throughput.