Randomness Assessment in Oscillator Based Elementary TRNG

Viktor Fischer, David Lubicz,
Florent Bernard, Nathalie Bochard

Abstract

Jittery clock signals produced in oscillators, particularly in ring oscillators are commonly used as a source of randomness in true random number generators (TRNG). The robustness of the generators, and hence their security, is closely linked to the entropy of the generated bit stream, which depends on the size of the jitter. Known jitter size can be used as an input parameter in a stochastic model for the estimation of entropy. Good entropy management can guarantee the security of the generator. We propose a simple precise method for measuring jitter that can be easily embedded in logic devices. It can be used to calibrate an oscillator based TRNG and/or for assessment of the entropy rate while the TRNG is in operation. The method was thoroughly evaluated in simulations and hardware tests and we show that despite its simplicity and small area requirements, it enables the jitter to be measured with an error of less than 5 %.