Oscillator based TRNG with a certified entropy rate

David Lubicz

Abstract

We describe a practical and efficient method to measure the entropy rate of a TRNG based on free running oscillators that does not require to output and analyse the clock signals with an external device. It rather relies on very simple computations, that can be embedded into any FPGA or ASIC with minor adaptation of classical designs. It can be used for the calibration of an oscillator based TRNG or to certify the entropy rate of a TRNG while in operation. Our approach, which is inspired by the coherent sampling method, works under the general hypothesis that the phase jitter is small compared to the period of the oscillators. In this case, we show that it is possible to measure the relative phase between two oscillators with a precision far higher than the time resolution given by the period of any internal clock signal. We use this observation to recover, under some reasonable heuristics, the distribution of the random walk component of the phase jitter from which it is possible to compute a lower bound of the entropy rate of the TRNG. Our method has been thoroughly tested with simulations and hardware implementations. We draw some conclusions and recommendations for a reliable implementation of TRNGs to be used for cryptographic applications.