An evaluation procedure for comparing clock jitter measurement methods

Arturo Mollinedo Garay

France

Keywords

Jitter measurement, True random number generator, Ring oscillators, Error analysis, Hardware implementation

Abstract

The source of randomness of a true random number generator (TRNG) needs to be monitored online as well as inside the device to guarantee unpredictability and hence security. Monitoring is accomplished by measuring the physical parameters of the generator that determine the entropy rate per bit of the output bitstream. The same parameters are usually used as inputs for the stochastic model. In the widely used oscillator-based TRNGs, one of the main parameters to be observed is the clock jitter. Several jitter measurement methods have been proposed in the last decade, but their precision and design constraints have not yet been objectively compared. We propose a simple yet useful methodology for the precise evaluation of jitter measurement methods including their design constraints. Our evaluation procedure relies on an analytical model of the jitter measurement method and simulations based on the model followed by stringent analysis of measurement errors. The new evaluation procedure was applied to four jitter measurement methods. The results clearly revealed differences in precision and in feasibility in hardware between the methods and confirmed the usefulness of the new approach.