On Ring Oscillator Based True Random Number Generators and Some of their Variants (Abstract)

Markus Dichtl

Siemens Corporate Technology

This talk will cover a variety of topics related to true random number generation with ring oscillators. In addition to classical ring oscillators, also some of their variations like Fibonacci-ring-oscillators will be considered. These variations will include a new TRNG design based on combinatorial multipliers available on some FPGA chips.

Various experimental confirmations of the results reported at Cryptarchi 2011 by Richard Newell in the presentation "Measurement of FPGA ring oscillator noise, and analysis using the Allan Variance method"will be given. The experimental results can only be explained by dependencies between ring oscillator jitter contributions which extend over longer ranges of time. As those dependencies with a long temporal range imply the existence of some memory mechanism, the talk will also suggest how this could work. This part of the presentation will be rather speculative and should be considered as a motivation for further research. Then it will become very concrete again by considering the necessary consequences from the ring oscillator jitter dependencies. One area, where consequences are clearly necessary, is the algorithmic post processing of the random bits, as most popular algorithms, like e. g. von Neumann post processing, are based on the assumption of statistically independent input bits.

The talk will also treat the interaction of ring oscillators and their variants with other circuits implemented on the same FPGA chip. There is experimental evidence for weak interaction of ring oscillators which is derived from measurements made completely on the FPGA chip. Finally, experimental results on the interaction of classical ring oscillators and Fibonacci ring oscillators with deterministic circuitry on the same FPGA will be presented.

Keywords: FPGA, true random number generator, ring oscillator, Fibonacci ring oscillator