A Temporal High Resolution Analysis of Ring Oscillator Behaviour Right After Restart (Abstract)

Markus Dichtl

The problem with true random number generation based on ring oscillators is that they produce both statistically dependent and independent jitter. In order to obtain random bits suitable for cryptographic purposes, a lower bound for the independent jitter is needed. A major step in this direction was the PhD thesis of Patrick Haddad: Caractérisation et modélisation de générateurs de nombres aléatoires dans les circuits intégrés logiques (Saint-Étienne, 2015).

The drawback of Haddad's work is that the jitter measurements only begin quite late after the restart of the ring oscillator. However, by the time jitter measurements start in the PhD thesis—approximately 30,000 ring oscillator periods after restart—dependent jitter is already very dominant, making it difficult to evaluate the independent contributions.

This paper presents a different approach to measuring the jitter of a ring oscillator of length 15 on an FPGA (as in the PhD thesis of Patrick Haddad). All inverters of the ring oscillator are sampled simultaneously every 10 ns, enabling high-resolution analysis of the phase of the ring oscillator and its temporal development. This method allows meaningful jitter measurements to begin as early as 500 periods after the restart of the ring oscillator.

The results obtained demonstrate that, for describing bits sampled from a ring oscillator immediately after restarting it, a stochastic model beyond the one proposed in Haddad's PhD thesis is needed.

As a collateral result, the visual representation of the measurements provides a very direct proof of the known fact that the durations of the two half-periods of a ring oscillator can be quite different.