

## Master de Recherche – Master of Research

Title: on-chip jitter measurement to improve the quality of oscillator-sampling based RNGs

Keywords: random number generator, jitter, oscillator sampling, VLSI, FPGA, VHDL

Contact: Olivier Sentieys (sentieys@irisa.fr)

Laboratory: IRISA/INRIA –CAIRN project-team (Lannion)

<http://www.irisa.fr/activity/research/cairn>

<http://www.irisa.fr/cairn>

The objective of a random number generator (RNG) is to produce random binary numbers that are statistically independent, uniformly distributed and unpredictable. RNGs are necessary in many applications like cryptography, communication, VLSI testing, probabilistic algorithms, and the number of systems requiring a high-quality hardware RNG is continuously increasing, specially in embedded circuits like Field Programmable Gate Array (FPGA) and System-on-Chip (SoC).

Generally, a hybrid RNG comprising a True Random Number Generator (TRNG) and a Pseudo Random Number Generator (PRNG) is used. PRNGs are based on deterministic algorithms. They are periodic, and must be initialized by a TRNG. TRNGs are based on a physical noise source (e.g. radioactive decay, thermal noise or free running jitter oscillators) and depend strongly on their implementation quality. Most of the TRNGs implemented in FPGA or SoC use phase jitter produced by a free running oscillator or a Phase-Locked Loop (PLL). Jitter is the deviation of a signal from its ideal behaviour. Jitter is caused by deterministic noise (power supply noise, cross-talk noise, pink noise) and by random noise (substrate noise, temperature) and strongly depends on the oscillator generator used in the TRNG (usually ring oscillator or PLL) [1]. In practice, jitter can be influenced by noise external to the FPGA (power supply noise, temperature) and by chip activity. This dependence is a weakness exploitable by exposing the TRNG in hostile environment conditions. Therefore, the objective of this Master's thesis is to study on-chip measurement of jitter to improve the quality of oscillator-sampling based RNGs.

Several methods exist for analyzing the jitter of an oscillator and the most conventional technique is based on the signal oversampling. However, to obtain sufficient accuracy (e.g. 100 ps), a fast clock is required (10 GHz). This therefore restricts the use of this technique. A second alternative is to convert a time measure into a digital scale with a Time-to-Digital Converter (TDC). A TDC circuit consists of a chain of delays, D flip-flops, counters and a reference clock with ideally no jitter. This clock is delayed by the chain of delay element representing the amount of jitter in the measured signal. For example, for a deviation of jitter 1ns and with a delay precision of 50 ps, at least 40 delay elements are required. The counter values correspond to the distribution function of jitter. The drawback is the circuit area that will strongly depend on the resolution. Optimizations of these "Vernier Delay Lines" have been proposed in [2] and, more recently, some FPGA architectures have also been proposed [3] thus opening new possibilities.

After bibliographic review of some methods for measuring jitter, the objective of this Master's thesis is to propose and implement new jitter on-chip measurement architectures suitable for FPGA and VLSI targets. This circuit will be part of an embedded TRNG component and will measure in real-time the jitter distribution in order to quantify its quality. Then, the designed on-chip jitter measurement will be compared against an external one, considered as a reference. Also, the study and the implementation of a Delay Locked Loop (DLL) maximizing the random jitter will be realized. This DLL will be part of the proposed on-chip jitter measurement.

A FPGA prototype and a VLSI chip will be designed.

## **Bibliography**

- [1] Amr M. Fahim, Clock Generators for SOC Processors: Circuits and Architectures, 2005, Springer-Verlag New York, Inc.
- [2] Antonio H. Chan and Gordon W. Roberts, A jitter characterization system using a component-invariant Vernier delay line, IEEE Trans. Very Large Scale Integr. Syst., 12-1, pp 79-95, 2004.
- [3] Favi, Claudio and Charbon, Edoardo, A 17ps time-to-digital converter implemented in 65nm FPGA technology, FPGA'09: Proceeding of the ACM/IEEE international symposium on Field programmable gate arrays, pp 113-120, Monterey, California, USA, 2009.