Asynchronous Self-Timed Rings for Randomness Generation

Abdelkarim Cherkaoui, Alain Aubert,
Viktor Fischer, Laurent Fesquet
Laboratoire Hubert Curien, Saint-Etienne, France

Abstract

Asynchronous self-timed rings are now considered as a promising solution for generating high-resolution timing signals. These oscillators seem to be more robust to temperature, voltage and process variability than the classic inverter based rings, thanks to an analog effect called the "Charlie Effect". Considering this, it appears that they are particularly suited for applications that need a certain level of security, especially randomness generation. Moreover, asynchronous self-timed rings possess inherent properties that make them fundamentally different from classic inverter rings: different oscillation modes, several transitions evolving in the ring simultaneously, several available phases etc.
In this presentation, we provide a framework to understand the fundamental properties of asynchronous self-timed rings. We also provide a comparison with classic inverter rings and give an insight into the possible use of these oscillators for randomness generation purposes.