Self-Timed Rings as Sources of Entropy

Abdelkarim Cherkaoui, Viktor Fischer, Alain Aubert
Hubert Curien Laboratory
18 rue Prof. Lauras, Saint-Etienne, France
Email: (abdelkarim.cherkaoui, fischer, alain.aubert)@univ-st-etienne.fr

Laurent Fesquet
TIMA Laboratory
46, Avenue Felix Viallet, Grenoble, FRANCE
Email: laurent.fesquet@imag.fr

Abstract—True Random Numbers Generators (TRNG) rely on a physical random process to generate random bit sequences. One of the most used random processes in digital devices is the jitter in clock signals. For a long time, Inverter Ring Oscillators (IRO) have been used to generate jittery clocks because they are easy to implement and have a high phase noise magnitude. On the other hand, recent studies on Self-Timed Rings (STR) showed that these oscillators are suitable for generating robust clock signals. In this paper, we analyse Self-Timed Rings as sources of entropy: we show that they provide a high quality random jitter suitable for TRNG design.

I. INTRODUCTION

Random Numbers Generators (RNG) are one of the basic blocks of cryptographic systems. They are used to generate encryption keys, initialization vectors, challenges and other seeds for cryptographic primitives. True Random Numbers Generators (TRNG) rely on a physical entropy source to generate random bit sequences. Jitter is obviously the most used and easily available physical random process in digital devices. One simple, and rather concise definition of jitter would be “the short-term variations of a digital signal’s significant instants from their ideal positions in time”, these variations are due to noise in electronic devices. Historically, the main technique to generate random numbers using jitter is to sample a jittery clock during its switching. The statistical quality of the generated bits is then determined by the jitter statistical properties. In fact, jitter should be unpredictable and uncorrelated to guarantee the security of the generated random bits. Authors of [1] analyze the jitter in clock signals and distinguish two main jitter components: a local Gaussian component which is random, and a global deterministic component which is predictable and can constitute a security threat for TRNGs. They point out the fact that in Inverter Ring Oscillators (IRO), jitter variations accumulate throughout the ring structure, but the local random component accumulates slower than the global deterministic component.

On the other hand, Self-Timed Rings (STR) are oscillating structures derived from asynchronous design techniques that are suitable for generating robust clock signals [2]. In section 2, we present the STR architecture and behavior; section 3 discusses and analyses the jitter profile in both IROs and STRs; section 4 confronts the analysis with experimental results and section 5 concludes the paper.
the ring stage propagation delay [4]. The Charlie effect causes events to push away from each other in time, leading them to spread evenly around the ring. An exhaustive description and model of STRs temporal behavior is presented in [2] and [4].

III. JITTER PROPAGATION IN IROs AND STRs

When dealing with ring oscillators, it is convenient to use the standard deviation of a population of measured oscillation periods as a measurement of the jitter magnitude, denoted \( \sigma_{\text{period}} \). Considering FPGA implementations of IROs and STRs, in both structures, each ring stage is implemented using one LUT (Look-Up-Table). \( \sigma_{\text{LUT}} \) is the standard deviation associated with the propagation delay of one LUT (independently of the function it implements). For the sake of consistency, we refer to \( \sigma_{\text{period}} \) as the period jitter and \( \sigma_{\text{LUT}} \) as the jitter of a LUT. The period jitter is determined by the jitter of one LUT -which is the same for both the IRO and STR- and the way it propagates in the ring structure. The following sections analyse jitter propagation in both IROs and STRs.

A. Jitter Classification

As explained in [1], two types of jitter must be considered when designing TRNGs:

- **Local Gaussian Jitter** - a pure random jitter which is generated locally in each LUT due to random noise sources (white noise, flicker noise ...). As a consequence of the Central Limit Theorem, the sum of these phenomena lead to a uniform normal distribution of the LUT propagation delay. This kind of jitter is suitable for TRNGs.

- **Global Deterministic Jitter** - a non-random jitter due to deterministic sources usually external to the ring structure, as power supply noise, environmental and deterministic fluctuations (temperature, electro-magnetic emanations ...). This kind of jitter is unwanted and extremely dangerous in TRNG design. In fact, it can be predicted and manipulated providing a backdoor for cryptographic attacks. Moreover, it can mask a low magnitude local Gaussian source making it hardly exploitable.

B. Jitter Propagation in IROs

The oscillation period of an IRO is defined by the required time for one event to achieve one lap around the ring structure. The event propagates freely across the ring: during its run, it accumulates jitter variations each time it crosses a ring stage. If we consider uncorrelated random noise (e.g. white noise), variances are additive. Therefore, if \( L \) is the number of ring stages:

\[
\sigma_{\text{period}} = \sqrt{L}\sigma_{\text{LUT}} \tag{2}
\]

For deterministic jitter, if \( D_{\text{det},i} \) is the deterministic contribution in the propagation delay of a LUT when the event crosses the stage \( i \), then the global deterministic contribution during one IRO period is:

\[
D_{\text{det}} = \sum_{i=1}^{L} D_{\text{det},i} \tag{3}
\]

Finally, jitter variations accumulate in IROs. However, deterministic jitter accumulates faster than the random jitter.

C. Jitter Propagation in STRs

In STRs, the oscillation period is defined by the elapsed time between two successive events crossing the same stage. However, the events propagation is constrained: separation times between the events converge to the functioning point of the steady regime that only depends on the static parameters of the STR. That suggests that jitter variations do not propagate in a STR. Therefore, in the case of uncorrelated random noise, we propose the following estimation of the period jitter of a STR, which is independent of the number of stages:

\[
\sigma_{\text{period}} \sim \sqrt{2}\sigma_{\text{LUT}} \tag{4}
\]

The STR architecture and behavior also suggests that global deterministic jitter is strongly limited in STRs. First, as for random jitter, deterministic jitter does not propagate because of the self-timed behavior. Secondly, since global deterministic variations affect each event with the same manner, they are attenuated because the period has a differential expression as the difference in the arrival moment of two successive events.

Finally, we suggest that jitter does not propagate in a STR. The detected jitter is mostly composed of the local Gaussian component generated in the ring stage serving as the oscillator’s output.

IV. JITTER MEASUREMENTS

In this section, we propose an experimental validation of our analysis in Altera Cyclone 3 and Xilinx Virtex 5 devices. Jitter measurement are provided using the statistical tools of a wide band digital oscilloscope LeCroy Wavepro 735 ZI (3.5GHz band and 40 Gsample/s). We used LVDS (Low Voltage Differential Signaling) interfaces and an active differential probe with a 4 GHz bandwidth. The boards feature a linear voltage regulator to mitigate deterministic effects due to the power supply.

A. Local Gaussian Jitter

Without external perturbations, both oscillators exhibit a Gaussian random jitter as shown in Fig. 2.

![Fig. 2. Period jitter histograms in Altera Cyclone 3 (a) 96-stage STR (b) 5-stage IRO](image)

We measured the period jitter for IROs with respect to the number of stages. As shown in Fig. 3, the period jitter of an IRO increases with the number of stages. The curve exhibits a square-root shape in high frequencies (low number of stages) and a linear shape in low frequencies. In fact, jitter in high frequencies is dominated by the uncorrelated random white noise (for which Equation (2) applies). While the jitter in low
frequencies is dominated by the flicker noise ($\frac{1}{f}$ noise), which is correlated because it depends on the frequency (Equation (2) do not apply here).

![Fig. 3. Period jitter of an IRO with respect to the number of stages](image)

In Fig. 4, we measured the period jitter of a STR with respect to the number of ring stages. $L$ the number of stages and $N$ the number of events are selected such as Equation (1) is verified. It appears that the period jitter is relatively constant (one measurement point differs with $2\, \text{ps}$ which is not significant) and does not depend on the number of ring stages. Moreover, Fig. 5 shows that the period jitter is also constant with respect to the ring occupancy. Which means that the self-timed behavior prevents jitter from propagating independently of the number of stages that separate events when they spread around the ring. Finally, the measurements suggest that the detected jitter corresponds to the local Gaussian component of the ring stage serving as the oscillator’s output.

![Fig. 4. Period jitter of a STR with respect to the number of stages](image)

![Fig. 5. Period jitter of a 64-stage STR with respect to the ring occupancy](image)

**B. Global Deterministic Jitter**

We propose a simple experiment to evaluate the influence of global deterministic jitter for both IROs and STRs. We implemented a 64-stage STR and a 7-stage IRO having nearby frequencies in an Altera Cyclone 3 device. A set of 512 3-stage IROs serve as a source of global deterministic jitter and can be enabled and disabled dynamically. These deterministic variations are mainly current peaks on the power supply rails that affect the propagation delay of the LUTs inside the device each time one of the perturbing rings switches. Fig. 6 shows the period distributions for the IRO and STR when the perturbation is enabled and disabled.

![Fig. 6. Period distributions of a 64-stage STR and a 7-stage IRO under the influence of deterministic effects](image)

It appears from Fig. 6 that the IRO’s period is not uniformly distributed when the perturbation is enabled, which suggests that it is affected by deterministic effects. On the contrary, the STR still exhibits a Gaussian period distribution when the perturbation is enabled. Therefore, the STR have a better rejection of deterministic effects than the IRO.

**V. CONCLUSION**

In this paper, we analysed jitter in IROs and STRs, showing that jitter propagates in the IRO structure while it does not in STRs. Even though jitter in STRs has a lower magnitude than in IROs, it also has a better quality because deterministic effects are strongly attenuated. Therefore, STRs provide a high quality random jitter suitable for TRNG design, constituting an interesting alternative for IROs as a source of entropy.

**ACKNOWLEDGMENT**

The presented research is funded by the Rhone-Alpes region (France) in the frame of the ISLE Cluster (Informatique, Signal et Logiciel Embarqué) and the SEMBA project (Systèmes EMBArqués).

**REFERENCES**


