

Comparison of Self-Timed Ring and Inverter Ring Oscillators as Entropy Sources in FPGAs

Abdelkarim Cherkaoui, Viktor Fischer, Alain Aubert, Laurent Fesquet

▶ **To cite this version:**

Abdelkarim Cherkaoui, Viktor Fischer, Alain Aubert, Laurent Fesquet. Comparison of Self-Timed Ring and Inverter Ring Oscillators as Entropy Sources in FPGAs. Design Automation and Test in Europe (DATE 2012), Mar 2012, Dresden, Germany. pp.1-6. ujm-00667639

HAL Id: ujm-00667639
https://ujm.hal.science/ujm-00667639

Submitted on 8 Feb 2012

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Comparison of Self-Timed Ring and Inverter Ring Oscillators as Entropy Sources in FPGAs

Abdelkarim Cherkaoui, Viktor Fischer, Alain Aubert
Hubert Curien Laboratory
18 rue Prof. Lauras, St.-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*—Many True Random Numbers Generators (TRNG) use jittery clocks generated in ring oscillators as a source of entropy. This is especially the case in Field Programmable Gate Arrays (FPGA), where sources of randomness are very limited. Inverter Ring Oscillators (IRO) are relatively well characterized as entropy sources. However, it is known that they are very sensitive to working conditions. This fact makes them vulnerable to attacks. On the other hand, Self-Timed Rings (STR) are currently considered as a promising solution to generate robust clock signals. Although many studies deal with their temporal behavior and robustness in Application Specific Integrated Circuits (ASIC), equivalent study does not exist for FPGAs. Furthermore, these oscillators were not analyzed and characterized as entropy sources aimed at TRNG design. In this paper, we analyze STRs as entropy sources for TRNGs implemented in FPGAs. Next, we compare STRs and IROs when serving as sources of randomness. We show that STRs represent very interesting alternative to IROs: they are more robust to environmental fluctuations and they exhibit lower extra-device frequency variations.**

I. Introduction

True Random Number Generators (TRNG) are ubiquitous in security chips, they are one of the basic cryptographic primitives. TRNGs are used to generate encryption keys as well as initialization vectors, challenges and signature parameters. Therefore, they must fulfill strict statistical requirements and be secure and unpredictable. The quality of the generated random sequence depends mainly on two factors: the quality of the entropy source and the entropy extraction method. While many TRNGs in ASICs use analog components to generate randomness, their realization in FPGAs is much more restricted. Currently, the majority of TRNGs on FPGAs rely on extracting the jitter from clock signals to generate random bit sequences. To achieve security requirements, the jittery clock signal needs to be precisely characterized.

Nowadays, IROs are the most widely used solution as generators of jittery clocks in both ASICs and FPGAs due to their low area, good integration in digital and analog design flow and important phase noise. However, previous studies showed that IROs are very sensitive to voltage and process variability. In [1], the authors present experimental results showing that changing operating conditions such as power supply voltage or operating temperature may affect the output quality of a ring oscillator based TRNG when the signal is subsampled. An attacker may subsequently shift the operating point via a simple non-invasive manipulation and easily bias the TRNG output. Another vulnerability is pointed out by the authors of [2] who analyze the jitter generated in ring oscillators and propose a simple physical model of jitter sources showing that the random jitter accumulates slower than the global and manipulable deterministic jitter.

978-3-9810801-8-6/DATE12/©2012 EDAA

On the other hand, STRs were studied in many contexts and seem to be a good alternative to IROs as generators of robust clock signals. Events in STRs can propagate evenly-spaced or as bursts. In [3], Winstanley et *al.* use Charlie diagrams to predict bursting behaviors in STRs. Hamon et *al.* carry on this study in [4]. They propose a high level time accurate model to predict the oscillation mode of a STR and provide simple design rules to prevent the burst oscillating mode. Moreover, they show by simulations that STRs offer better robustness to process variability than IROs.

Our study of STR was motivated by the fact that most of previous works were oriented in ASICs and equivalent study does not exist for FPGAs. Furthermore, while a wide range of oscillators was characterized and used in TRNGs, still no study deals with the possible use of STRs as randomness sources.

This paper extends the works presented in [4]. Our experimental results confirm robustness of STRs in FPGAs. The paper also provides a characterization of STRs as entropy sources and compares STRs with IROs. It is organized as follows: Section 2 describes the architecture and behavior of STRs and IROs. Section 3 defines the temporal model for STRs adopted in this paper. Section 4 analyses the jitter in both STRs and IROs. Section 5 regroups and discusses the experimental results obtained in FPGAs. Section 6 concludes the paper.

II. Rings Architecture and Behavior

This section presents the studied rings architecture and behavior and describes the analog effects that influence the propagation delay of a STR stage.

A. IRO Architecture and Behavior

The studied IRO structure is depicted in Fig. 1. The first ring stage is an inverter while all other stages are delay elements.

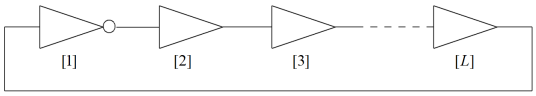


Fig. 1. Studied IRO architecture

L ring stages are connected to form a ring. The oscillatory behavior of the IRO is due to the propagation of one event all around the ring: each ring stage propagates the rising and falling edge of the generated clock signal in two successive half-periods [2].

B. STR Architecture

The STR structure is depicted in Fig. 2. It corresponds to the control path of a micropipeline as proposed by I. E. Sutherland in [5], which was closed to form a ring of L stages. Each stage is composed of a Muller gate and an inverter. For the stage i, F_i is the forward input, R_i the reverse input, and C_i is the output.

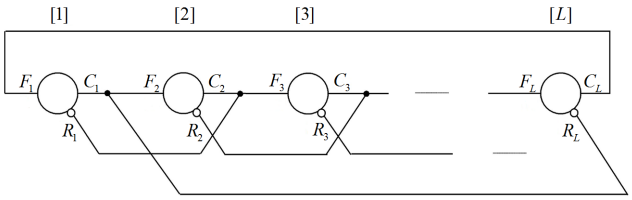
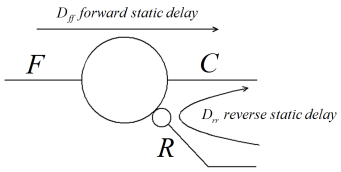


Fig. 2. Architecture of a self-timed ring

Fig. 3 shows the truth table of a stage. The forward input value is written to the output if the forward and reverse input values are different, otherwise previous output is maintained.



F	R	C
0	0	C^{-1}
0	1	0
1	0	1
1	1	C^{-1}

Fig. 3. Ring stage structure and truth table

C. STR Behavioral Model

1) Bubbles and Tokens: The tokens and bubbles concept is derived from a 2-phase communication protocol as described in [5]:

- Stage i contains a bubble if its output C_i is equal to the output of the previous stage C_{i-1}

$$C_i = C_{i-1}$$

- Stage i contains a token if its output C_i is different from the output of the previous stage C_{i-1}

$$C_i \neq C_{i-1}$$



Fig. 4. Propagation of tokens and bubbles in STRs (tokens move to the right, bubbles to the left)

2) Tokens and Bubbles Propagation: Knowing the stage truth table and the token and bubbles concept described above, a token propagates from the stage i to the stage $i+1$ if and only if the next stage $i+1$ contains a bubble (see Fig. 4). In the same time, a bubble propagates from the stage $i+1$ to the previous stage i if and only if the previous stage i contains a token. The condition for a token to propagate from stage i to stage $i+1$ is expressed as follows:

$$C_i \neq C_{i-1} \; and \; C_i = C_{i+1}$$

The propagation rule implies STR will have an oscillatory behavior if the next conditions are valid:

- $L \geq 3$, $L = N_T + N_B$,
- $N_B \geq 1$, where N_B is the number of bubbles,
- N_T is a positive even number of tokens.

3) Steady Regime: STRs can evolve into two propagation modes: an evenly-spaced and a burst propagation mode [3] (see Fig. 5). The evenly-spaced mode occurs when the tokens evenly spread all-around the ring and propagate with a constant spacing. The burst mode occurs when the tokens get together to form a cluster that propagates all around the ring. The oscillation mode in the steady regime depends on the stage timing parameters and the ratio N_T/N_B [4].

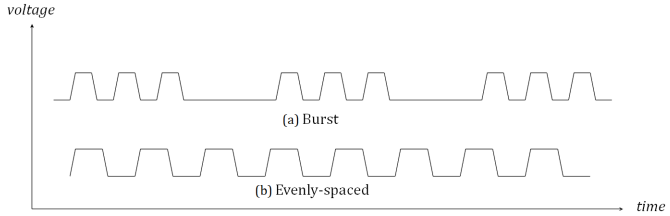


Fig. 5. Burst and evenly-spaced propagation modes in STRs

D. The Drafting and Charlie Effects

Recognizing that the propagation delay of a Muller gate depends on the relative arrival times of the input events, Ebergen et *al.* proposed for the first time in [6] the use of Charlie diagrams to predict the output delay of a Muller gate. The model proposed in [3] allows to take into account two analog phenomena that affect the propagation delay of a ring stage: the Charlie and drafting effects.

1) The Charlie Effect: Previous works on the C-element (Muller gate) point out the impact of the separation time between input events on a STR stage propagation delay: the closer are the inputs arrival times, the longer will be the stage propagation delay.

2) The Drafting Effect: The drafting effect describes the impact of the elapsed time from the last output event on a gate propagation delay: the shorter is this time, the shorter will be the gate propagation delay. While the drafting effect can easily be determined and relatively be strong in ASICs, our experience shows that this effect is much lower in FPGAs. Therefore we propose to neglect the drafting effect in our study.

3) Evenly-spaced Mode Locking Mechanism: The Charlie effect is the key to understand how a STR evolves into the evenly-spaced propagation mode. When two tokens get closer in the ring, the separation time of a ring stage is shorter and the propagation delay is thus longer due to the Charlie effect. That means that, under the influence of the Charlie effect, tokens push away from each other, which makes them spread evenly all around the ring. The authors of [4] proved that it is possible to guarantee the evenly-spaced propagation mode by respecting a simple design rule without any knowledge of the Charlie effect parameters:

$$\frac{N_T}{N_B} = \frac{D_{ff}}{D_{rr}}, \tag{1}$$

where D_{ff} is the forward static delay and D_{rr} the reverse static delay of a ring stage as depicted in Fig. 3. For randomness generation purposes, we consider that the burst oscillation mode is irrelevant since it could introduce an undesirable bias to the generator. In our characterization of STRs, we focus on the evenly-spaced propagation mode, which can be set by adjusting the ratio N_T/N_B at the ring initialization.

III. STR Temporal Model

We propose in this section to clearly define the initial hypothesis in order to establish the Charlie model for studied implementations of STRs in Altera FPGAs. This model provides a framework for understanding the robustness properties and the jitter characteristics of the studied rings.

A. Initial Hypothesis

Considering that each STR stage is implemented in one Look-Up-Table (LUT) and the interconnection delays are neglected, we can assume that $D_{ff} = D_{rr}$. Consequently, according to Equation 1, STRs initialized with as many tokens as bubbles should evolve into the evenly-spaced propagation mode. For the rest of our study:

$$N_T = N_B \tag{2}$$

B. Charlie Diagram

The Charlie diagram gives the propagation delay of a ring stage as a function of the separation time between the input events, while taking into account the Charlie effect. It is tuned in our case by 2 parameters:

- D_s – the static propagation delay of a ring stage,
- $D_{charlie}$ – the Charlie effect magnitude.

Fig. 6 represents an example of a timing diagram of one STR stage. An example of a Charlie diagram is plotted in Fig. 7. The shape of the Charlie diagram fits a parabola inscribed in the straight lines $D_s - s$ and $D_s + s$. The analytical Charlie equation is expressed as follows:

$$charlie(s) = D_s + \sqrt{D_{charlie}^2 + s^2} \tag{3}$$

It can be observed that the shorter is the separation time s the smaller is the derivative $\frac{dcharlie}{ds}$. That means that variations around $s = 0$ (bottom of the curve) are smoothed

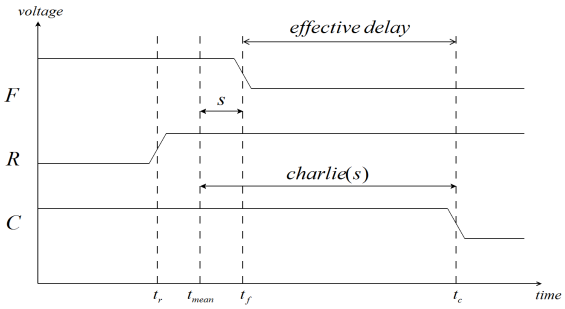


Fig. 6. Ring stage timing diagram

thanks to the Charlie effect. If the Charlie effect magnitude $D_{charlie}$ is more important, the interval around $s = 0$, where the derivative $\frac{dcharlie}{ds}$ is small, becomes larger and variations are smoothed to a bigger extent. In conclusion, two factors influence the robustness properties of STRs: the magnitude of the Charlie effect, and the separation time for each ring stage in the steady regime. Ideally, and according to the time accurate model presented in [4], a STR with $N_T = N_B$ and $D_{ff} = D_{rr} = D_s$ would have null separation times in the steady regime for each ring stage with a maximal Charlie effect.

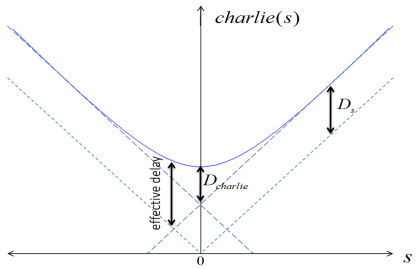


Fig. 7. Example of a Charlie diagram

IV. Analysis of the Jitter in STRs and IROs

We propose in this section a simple jitter model for the studied STRs and IROs. As explained in [2], two types of jitter must be considered in TRNGs: local Gaussian jitter (the source of randomness), and global deterministic jitter (a mean for attacking the generator). One of the jitter measurements is the period jitter. The period jitter is defined as the deviation of the oscillation period T from its ideal value T_{id} (or mean value T_{mean}). The standard deviation σ_{period} of a population of measured periods is often used to quantify the period jitter. For the sake of consistency, we refer to σ_{period} as the period jitter.

A. Local Gaussian Jitter

In the studied FPGA implementation of STR and IRO, each ring stage (which is implemented in one LUT for both IRO and STR) is considered as a source of the local Gaussian jitter: its propagation delay follows a normal distribution $\mathcal{N}(D_g, \sigma_g^2)$. We refer to σ_g as the jitter of a single gate (LUT cell).

The major difference in period jitters of STRs and IROs lies in the way the jitter accumulates throughout the structure. In the IRO, the period is defined by two laps of one event all

around the ring structure. During its run, the event accumulates the jitter with a square root law with respect to the number of the crossed stages. Thus, the period jitter σ_{period} can be expressed as a function of the number of stages (k) and the jitter of one gate (σ_g):

$$\sigma_{period} = \sqrt{2k}\sigma_g \quad (4)$$

In a STR, several events propagate in the ring simultaneously: each token is an event propagating across the ring. The oscillation period is defined by the elapsed time between successive tokens. Each token crossing a stage experiences a variation in its propagation delay due to the local Gaussian jitter contribution of the stage. For example, if token i reaches stage k at the time $t_{k1}+\mathcal{N}(0,\sigma_g^2)$, and token $i+2$ reaches stage k at the time $t_{k2}+\mathcal{N}(0,\sigma_g^2)$, the elapsed time between the two tokens is $t_{k2}-t_{k1}+\mathcal{N}(0,2\sigma_g^2)$. Contrary to IRO, the effect of jitter accumulation is only temporary since the Charlie effect permanently regulates the tokens temporal spacing. Therefore, we can approximate $t_{k2}-t_{k1}$ by a constant equal to the mean oscillation period T_{mean}. Subsequently, we estimate the period jitter, which is independent of the number of stages as follows:

$$\sigma_{period} \sim \sqrt{2}\sigma_g \quad (5)$$

Finally, we suggest that the period jitter in STRs is mostly composed of the jitter generated locally in the ring stage serving as the output of the oscillating signal.

B. Global Deterministic Jitter

Global deterministic jitter refers to the non-random variations in propagation delays due to external global influences (e.g. a modulation of the power supply voltage). The authors of [2] pointed out the fact that global deterministic jitter accumulates linearly throughout the IRO structure. If D_{det_i} is the deterministic contribution in the propagation delay when the propagating event crosses stage i, then $D_{det} = \sum_{i=1}^{2k} D_{det_i}$ is the global deterministic contribution during one IRO period. Here again, the main difference with the STR is the fact that in the STR several events propagate simultaneously. When a deterministic variation is applied to the ring, it affects each event in the same way. Since the half-period is defined by the elapsed time between two successive events, we suppose that the deterministic term is strongly attenuated. On the other hand, the deterministic delay variations are smoothed as the Charlie effect regulates the token propagation.

V. Experimental Results

In order to validate our analysis, we used five equivalent boards designed especially for TRNG applications and featuring Altera Cyclone III devices. To reduce deterministic jitter introduced by the power supply, these boards also feature a linear voltage regulator. Frequency and jitter were measured externally using a wide band digital oscilloscope LeCroy Wavepro 735 ZI. In order to reduce the impact of the slow standard input/output circuitry, we used the LVDS (Low Voltage Differential Signaling) interface of the device and an active differential probe with a 4 GHz bandwidth.

A. Observations, remarks

We implemented several configurations of IROs and STRs in the selected FPGAs. Logic cells were placed manually (if possible in the same Altera LAB) in order to reduce the interconnection delays. We verified experimentally that STRs with $N_T = N_B$ evolve into the evenly-spaced mode for ring lengths varying from 4 to 96. Furthermore, experiment shows that for a 32-stage ring, evenly-spaced mode is obtained for configurations where $N_T = \{10, 12, 14, 16, 18, 20\}$ which suggests a high charlie effect in the selected devices.

B. Sensitivity to Voltage Variations

We measured ring frequencies for core power supply voltage varying from $1V$ to $1.4V$. Frequencies are normalized to compare Robustness to Voltage Variations (RVV) between oscillators that have different frequencies:

- F being the measured frequency at various voltage levels and F_{nom} the measured frequency at $1.2V$, the normalized frequency F_n is expressed as follows
$$F_n = \frac{F}{F_{nom}}$$
- F_{max} being the measured frequency at $1.4V$ and F_{min} the measured frequency at $1V$, the normalized frequency excursion ΔF is defined for a $0.4V$ voltage sweep as follows
$$\Delta F = \frac{F_{max}-F_{min}}{F_{nom}}$$

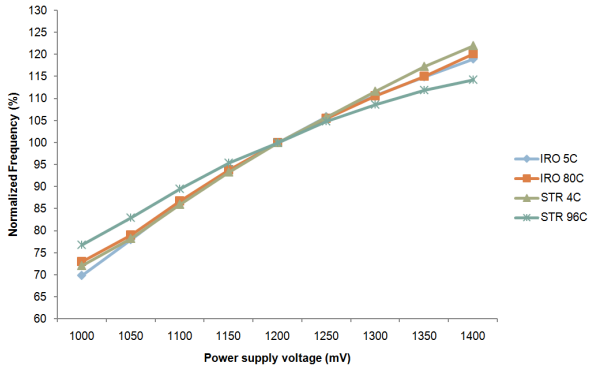


Fig. 8. Normalized Frequencies for core power supply varying from $1V$ to $1.4V$

Fig. 8 shows the normalized frequencies for different ring configurations: IROs with 5 and 80 stages, STRs with 4 and 96 stages. According to these measurements, frequencies vary linearly with voltage, and the 96-stage STR exhibits a lower voltage sensitivity than other ring configurations.

We note the 4-stage STR achieves the same sensitivity to voltage variations than the IRO configurations. In reality, due to routing delays, separation times can occur in the linear part of the Charlie diagram in Fig. 7 where the Charlie effect is neglectable. However, Table I shows that RVV is slightly improved for the STR when we increase the number of stages, which is not the case for the IRO. Although the adopted temporal model does not explain this fact, we suggest that a higher number of stages causes tokens to be more constrained in the structure: this issue is a research area that needs to be explored.

TABLE I
NORMALIZED FREQUENCY EXCURSIONS FOR A 0.4 V VOLTAGE SWEEP AROUND NOMINAL VOLTAGE 1.2 V

Ring	F_n (Mhz)	ΔF
IRO 5C	376	49 %
IRO 25C	73	48 %
IRO 80C	23	47 %
STR 4C	653	50 %
STR 24C	433	44 %
STR 48C	408	39 %
STR 64C	369	39 %
STR 96C	320	37 %

Finally, while IROs RVV cannot be improved by design, it is possible to increase STRs RVV at the cost of a larger FPGA logic resources usage.

C. Sensitivity to Process Variability

Process variability refers to the extra-device variability of propagation delays, which is due to the technology and manufacturing process. In this section, we evaluate the extra-device frequency variability for different ring configurations by sending the same bit-stream to five available boards. For each ring, we measured the ring frequencies in each board and calculated the relative standard deviation σ_{rel} as follows:

$$\sigma_{rel} = \frac{\sigma}{F_{mean}}$$

where σ is the standard deviation of the measured frequency values and F_{mean} is the mean of the measured frequency values. Results are presented in Table II.

TABLE II
RELATIVE STANDARD DEVIATION OF FREQUENCY VALUES FOR DIFFERENT OSCILLATORS IMPLEMENTED IN 5 DEVICES

Ring	Frequency (Mhz)					σ_{rel}
	board 1	board 2	board 3	board 4	board 5	
IRO 3C	654.42	646.84	641.56	645.60	642.12	0.79 %
IRO 5C	305.72	306.44	302.54	304.87	302.20	0.62 %
STR 4C	669.05	660.06	658.60	659.90	655.62	0.76 %
STR 96C	328.16	328.54	327.55	328.47	327.46	0.15 %

According to Table II, the frequency dispersion of the 96-stage STR is narrower than for other rings. Here again, it appears that increasing the number of stages improves the robustness of STRs against the process variability. One can argue that this is also true for IROs, because increasing the number of stages allows to approach more accurately the mean propagation delay of a ring stage. However, while it is possible to maintain high frequencies in STRs, frequency decreases linearly with the number of stages in IROs. Therefore, STRs achieve much better robustness to extra-device frequency variability at high frequencies than IROs.

D. Jitter Measurements

Jitter measurements in this section are provided using the wide-band digital oscilloscope LeCroy Wavepro 735 ZI statistical tools.

1) Jitter Histograms: Fig. 9 shows the period jitter histograms for a 96-stage STR and a 5-stage IRO with similar frequencies (around 300 MHz). Both the IRO and STR exhibit a Gaussian jitter. This is not a new result for IROs, but it is relevant for STRs. The Gaussian jitter distribution in STRs

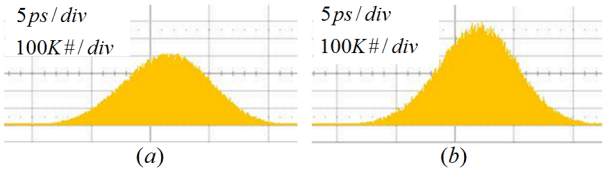


Fig. 9. Period jitter histograms (a) 96-stage STR (b) 5-stage IRO

makes self-timed rings interesting for jittery clock generation in TRNGs. We verified this fact for rings of up to 96 stages (with $N_T = N_B$).

2) Jitter Measurement Method: Although the oscilloscope could theoretically measure the period jitter and the cycle-to-cycle jitter (difference between two successive periods), it was not suitable for precise measurements of very low jitter values that were biased due to the error introduced by the the sampling frequency of the oscilloscope and the input/output circuitry. Therefore, we measured the accumulated jitter and computed the initial jitter values using the theoretical jitter accumulation properties presented in [2]. osc is the output of the ring oscillator. Signal osc_mes is generated inside the chip by counting $2n$ rising events of signal osc as depicted in Fig. 10. The idea is to measure osc_mes jitter values and to compute osc jitter values.

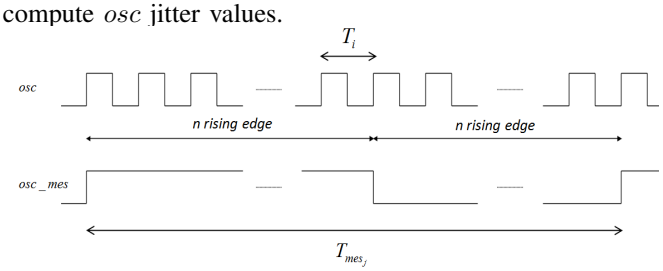


Fig. 10. Jitter measurement method scheme

osc_mes period is expressed as follows:

$$T_{mes_j} = \sum_{k=1}^{2n} T_i$$

The ring oscillator period can be decomposed into a random and a deterministic contribution. The random term follows a normal distribution $\mathcal{N}(T_{mean}, \sigma_p^2)$ where T_{mean} is its mean and σ_p^2 is its variance. D_i is the deterministic contribution during the period i of osc:

$$T_i = \mathcal{N}(T_{mean}, \sigma_p^2) + D_i$$

When adding independent random variables, variances are added:

$$T_{mes_j} = \mathcal{N}(2nT_{mean}, 2n\sigma_p^2) + D_{det_j}$$

where $D_{det_j} = \sum_{k=1}^{2n} D_i$ is the deterministic contribution during a period of signal osc_mes.
The main hypothesis of the method proposed in this section is expressed as follows: It is always possible to choose n high enough to verify the following assumption:

$$D_{det_{j+1}} - D_{det_j} \ll 4n\sigma_p^2$$

We systematically verify this hypothesis before applying the method by simply checking the cycle-to-cycle period histogram of signal osc_mes and verifying that it follows a

normal distribution. Therefore, the difference between two successive osc_mes periods is:

$$\triangle T_{mes} \simeq \mathcal{N}(0, 4n\sigma_p^2)$$

Using the oscilloscope, we measure the cycle-to-cycle jitter $\sigma_{mes_{cc}}$ of signal osc_mes. Finally:

$$\sigma_p = \frac{\sigma_{mes_{cc}}}{2\sqrt{n}} \quad (6)$$

In the case of IRO, and according to equation 4, we can deduce the standard deviation (σ_g) related to the jitter generated locally in a single LUT cell (k being the number of stages):

$$\sigma_g = \frac{\sigma_p}{\sqrt{2k}} \quad (7)$$

3) Results: We measured period jitter for both the IRO and STR as a function of the number of stages. In Fig. 11, we plotted the period jitter σ_p for the IRO with respect to the number of stages. For each measured value, we computed and plotted σ_g the standard deviation of a single gate propagation delay.

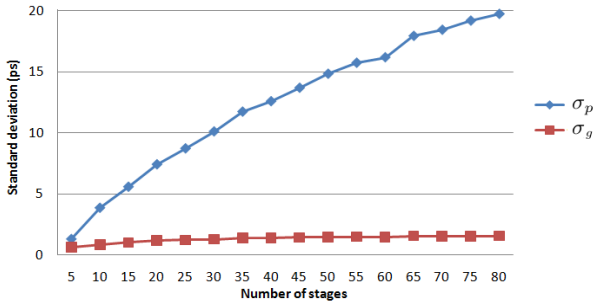


Fig. 11. Period jitter of an IRO with respect to the number of stages

The curve shows a square-root accumulation tendency which verifies Equation 4. Moreover, we could estimate σ_g:

$$\sigma_g \simeq 2ps$$

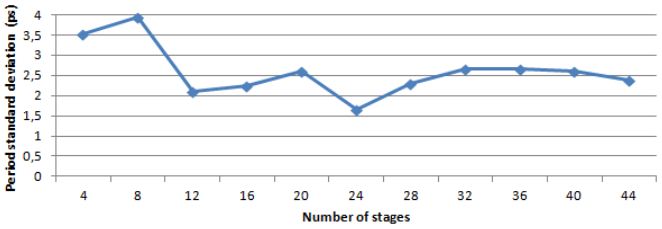


Fig. 12. Period jitter of a STR with respect to the number of stages

In Fig. 12, we plotted the period jitter σ_p for the STR as a function of the number of stages. The measured values are relatively constant with respect to the number of stages (between $2ps$ and $4ps$) as expected considering the analysis in Section IV-A. Moreover, the measured values converge to a constant value when we increase the number of stages. As for robustness to voltage variations, this result suggests that tokens are more constrained and the Charlie effect is more present in this case. In addition, $\sqrt{2}\sigma_g \simeq 2.83ps$ which corresponds to the constant value of σ_p for high number of stages ($\sim 2.5ps$). Finally, these measurements confirm Equation 5 proposed in Section IV-A.

VI. Conclusion

In this paper, we compared inverter ring oscillators and self-timed rings when serving as entropy sources:

- we evaluated and compared robustness to voltage and device manufacturing process variability for both IROs and STRs,
- we analyzed the jitter in STRs and validated our analysis experimentally by jitter measurements.

The results showed that the robustness of STRs to voltage variations can be enhanced by increasing the ring length, which is not the case for IROs. STRs exhibit also lower extra-device frequency variations than their counterparts when operating in high frequency ranges. The period jitter in STRs does not depend on the ring length, but mostly on the local jitter generated in one ring stage, which means that each ring stage can be considered as an independant entropy source. Even though their gaussian jitter can be lower than in IROs, STRs exhibit a lower deterministic jitter. We can therefore suppose that STR-based TRNGs should be more robust to attacks than IRO-based TRNGs. In addition, STRs robustness to manufacturing process variability is a feature that can be successfully used in many TRNG designs and namely in TRNGs based on the coherent sampling [7], where the designer needs to guarantee that the ring oscillators frequencies will remain in a required interval for all devices of the same family. Our future works will focus on exploiting the STR properties for designing a robust TRNG.

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

[1] S. K. Yoo, D. Karakoyunlu, B. Birand, and B. Sunar, "Improving the Robustness of Ring Oscillator TRNGs," in ACM Transactions on Reconfigurable Technology and Systems (TRETS), Volume 3, 2010.

[2] V. Fischer, F. Bernard, N. Bochard, and M. Varchola, "Enhancing Security of Ring Oscillator-based RNG implemented in FPGA," in Field-Programable Logic and Applications (FPL), pp. 245–250, 2008.

[3] A. Winstanley and M. R. Greenstreet, "Temporal Properties of Self-Timed Rings," in Proceedings of the 11th Advanced Research Working Conference on Correct Hardware Design and Verification Methods, CHARM01. London, UK: Springer-Verlag, pp. 140–154, 2001.

[4] J. Hamon, L. Fesquet, B. Miscopein, and M. Renaudin, "High-Level Time-Accurate Model for the Design of Self-Timed Ring Oscillators," in Proceedings on the 14th International Symposium on Asynchronous Circuits and Systems, ASYNC08, Apr. 2008, pp. 29–38.

[5] I. E. Sutherland, "Micropipelines," Communications of the ACM (Association of Computing Machinery), Vol/Issue: 32/6, pp. 720–738, 1989.

[6] J. C. Ebergen, S. Fairbanks, and I. E. Sutherland, "Predicting Performance of Micropipelines Using Charlie Diagrams," in Proceedings of the Fourth International Symposium on Advanced Research in Asynchronous Circuits and Systems, ASYNC98, pp. 238–246, 1998.

[7] B. Valtchanov, V. Fischer, and A. Aubert, "Enhanced TRNG based on the coherent sampling," International Conference on Signals, Circuits and Systems (SCS), 2009.