Impact of the flicker noise on the ring oscillator-based TRNGs

Licinius Benea, Mikael Carmona, Viktor Fischer, Florian Pebay-Peyroula, Romain Wacquez

IACR Transactions on Cryptographic Hardware and Embedded Systems
ISSN XXXX-XXXX, Vol. 0, No. 0, pp. 1–20. DOI:XXXXXXXX

Impact of the Flicker Noise on the Ring Oscillator-based TRNGs

Licinius Benea[1], Mikael Carmona[1], Viktor Fischer[3,4], Florian Pebay-Peyroula[1] and Romain Wacquez[1,2]

[1] Univ. Grenoble Alpes, CEA, LETI MINATEC Campus, F-38054 Grenoble, France
(licinius-pompiliu.benea,mikael.carmona,florian.pebay,romain.wacquez)@cea.fr
[2] CEA-Leti, Mines Saint-Étienne, Equipe Commune, F-13541 Gardanne, France
[3] Hubert Curien Laboratory, Jean Monnet University, Saint-Etienne, France,
fischer@univ-st-etienne.fr
[4] Faculty of Information Technologies, Czech Technical University, Prague, Czech Republic,
viktor.fischer@fit.cvut.cz

Abstract. Ring Oscillators (RO) are often used in true random number generators (TRNG). Their jittered clock signal, used as randomness source, originates from thermal and flicker noises. While thermal noise jitter is generally used as the main source of randomness, flicker noise jitter is not due to its autocorrelation. This work aims at qualitatively settling the issue of the influence of flicker noise in TRNGs, as its impact increases in newer technology nodes. For this, we built a RO behavioural model, which generates time series equivalent to a jittered RO signal. It is then used to generate the output of an elementary RO-TRNG. Despite general expectations, the autocorrelation inside the output bit stream is reduced when the amplitude of flicker noise increases. The model shows that this effect is caused by the sampling of the jittered signal by the second oscillator, which hides the behaviour of the absolute jitter, causes resetting of the perceived phase, and suppresses any memory effect. The inclusion of flicker noise as a legitimate noise source can increase the TRNG output bit rate by a factor of four for the same output entropy rate. This observation opens new perspectives towards more efficient stochastic models of the RO-TRNGs.

Keywords: Random number generation · Parameterized stochastic models · Dedicated statistical tests · Physical isolation · Hardware monitoring

1 Introduction

Recent multiplication of attacks on IoT devices pushes security standards towards stronger requirements on security primitives. As such, True Random Number Generators (TRNG), which ensure the unpredictability of cryptographic secrets, are based on a physical source of randomness (usually some kind of analog noise), which is monitored and digitized to obtain a digital noise [AATS17]. The statistical quality of the generated digital noise is then verified using statistical tests [TBK+18], [KS11]. This statistical evaluation of the raw random numbers is necessary, but not sufficient: their origin, quality and unpredictability must be proven through a comprehensive and reliable stochastic model. Such a model serves to estimate the entropy rate at generator's output depending on measurable input physical parameters. So far, ring oscillators (RO) are one of the most studied and exploited sources of randomness [BLMT11, KG04, SMS07, VD10, HFBN15] in digital devices. The RO-based TRNGs exploit the jittered clock signal generated by the freely running oscillator. The jitter of the generated clock signal (i.e. instability of the signal in time), which is observed as a phase noise in frequency domain or a timing jitter in the time domain,

is caused by an ensemble of electric noises and in particular by random noises such as thermal noise and flicker noise. This variation in phase or in time of the clock signal is then transformed to a digital noise using a sampling or counting method [ASP+18] after sufficiently long jitter accumulation time. The stochastic models used to estimate entropy must be based on a detailed analysis of the underlying physical phenomena. Namely, in the context of RO-based TRNG, this necessitates a thorough study of the jitter origin, its size and the way it is accumulated.

Hajimiri *et al.* proposed one of the first comprehensive models of the jitter [HLL99]. It is based on the observation that the impact of a perturbation (noise) on the jitter is different whether this occurs during the transient phases (rising or falling edges) or the steady state phases of the clock signal. Consequently, the authors in [HLL99] define an Impulse Sensitivity Function (ISF), which characterizes the sensitivity of the signal to perturbations occurring at different instants. More precisely, the model describes the physical sources of the jitter, namely the thermal noise and flicker noise and their influence on the accumulated jitter. They conclude that the thermal noise is completely random and uncorrelated. This makes it an ideal source of randomness in TRNG applications. On the other hand, flicker noise originates from two major phenomena: carrier number fluctuation due to presence of traps at the interface between the gate oxide and the silicon channel, and mobility fluctuation due to Coulomb scattering in the channel of the transistor [GRND+91]. This type of the jitter source introduces correlations (namely auto-correlations) and might reduce the quality of generated numbers if the generator relies on it as a source of randomness.

The authors in [HLL99] prove that the variance of the accumulated jitter varies linearly in the case of jitter coming from the thermal noise (this jitter component is thus predominant in short accumulation times) and quadratically for the jitter coming from the flicker noise (the corresponding component of the jitter will thus be predominant in long accumulation times). Abidi [Abi06] proposes a model which is based on the physical parameters characterizing transistor noise models. However, this model cannot be used to determine the dependence of the jitter on the flicker noise due to divergence problems related to the flicker noise. Haddad *et al.* [HTBF14] propose to solve the convergence problem by recurring to the Allan variance [All66] instead of the traditional variance when analysing the sources of jitter. The accumulated jitter is characterized by the variance of the number of oscillations of one ring during N periods of the second one. The Allan variance calculated using the counter values follows a law similar to the one of Hajimiri *et al.*, which depends linearly on the jitter coming from thermal noise (jitter component predominant for low N) and quadratically on the jitter coming from flicker noise (jitter component predominant for higher N). Allini *et al.* [ASP+18] arrive to the same conclusions, by modifying the structure of the block calculating the variance. Another model proposed by Fischer and Lubicz [FL14] uses the digital output of a differential pair of ROs connected directly to a D flip-flop. An XOR operation is performed at the output, which depends on the differences between consecutive samples distanced by M bits. The proposed method is based on the autocorrelation test. The objective is to shorten the measurement interval and measure the jitter in the time domain in which the impact of the thermal noise dominates.

The relationship between the jitter coming from the thermal noise and entropy in oscillator-based TRNG was developed in [BLMT11]. By using a phase-oriented approach, the formula for a minimum boundary of entropy is provided. The entropy can be calculated from the quality factor of the oscillator, which depends on the ratio between the purely random jitter and the period of the oscillator. However, as yet, only the jitter coming from the thermal noise was taken into consideration even though the flicker noise is always present in an either consistent or dominant amount [BCPPW22]. The impact of the flicker noise is neglected because of its intrinsic autocorrelated behaviour, which is considered

to be a possible cause of predictability of the TRNG output. In order to investigate the influence of the flicker noise on the working characteristics of the TRNG, we model the behaviour of ring oscillators and furthermore of a TRNG by a behavioural model coded in Python. For ease of language, the behavioural model is referred to sometimes in this article as the emulator. The main purpose of the emulators is to emulate generated output signals of the ring oscillator. These signals are then used to evaluate the behaviour of the whole TRNG. Finally, we compare signals obtained from the emulator with those obtained from the dedicated hardware to adjust precisely the amplitude and impact of both noise sources on the emulator output. This allowed us to test and highlight the influence of the two noise sources separately and especially to evaluate the possibility to include the flicker noise effect on the final entropy rate and thus significantly increase the entropy rate.

The paper is organised around the following structure. The second section is dedicated to the description of the behavioural model of the RO. In this part, we describe the model and assumptions on which it is based and we validate the model by comparing model-generated and measured data coming from the dedicated hardware (ASIC and FPGA). This part also contains a study of the importance of parameters of the sampling process and namely the sampling frequency for jitter characterization. In the third section, we extend our study to an Elementary RO TRNG. The influence of the different noise sources on the working characteristics of a ring oscillator-based TRNG is studied. More explicitly, we explain the influence of the flicker noise on the TRNG behaviour, answering in this manner the question about its suitability as a source of randomness in physical random number generators.

2 Ring oscillator behavioural model

The purpose of this part is to provide a simple and effective way of generating a ring oscillator-type signal specifically designed for TRNG applications. More precisely, our emulator, which is written in Python, is able to generate time series corresponding to the rising (or falling) edges of a ring oscillator signal. A more detailed motivation is given in Section 2.2.

2.1 Model and hypothesis

In order to construct the behavioural model of jitter in ring oscillators, we use the results of the study of Hajimiri *et al.* from which most jitter models are derived [HLL99]. This model is based on the observation that the impact of a perturbation event (noise) on jitter is different whether it occurs during the rising (or falling) edge or the steady state phase of the signal. In the former case, the impact is important, while for the latter case the impact is negligible. This difference is represented by the Impulse Sensitivity Function (ISF), which translates the sensitivity of the signal to perturbations occurring at different instants. Thus, the ISF is either positive or negative during the rising or falling edges of the signal and null in the steady state part (see Fig. 1).

The absolute phase is calculated by integrating the product between the ISF (Γ) and the current noise coming through the inverter levels of the ring oscillator, all divided by a constant charge q_{max}, which is characteristic to each ring oscillator (see Eq. 1). One can observe that the cumulative sum is composed of essentially two terms. The first one, $\frac{\Gamma(\omega_0\tau)}{q_{max}}$ is an amplitude term describing the impact of a variation of current on the phase noise. The second term, $i(\tau)$, is the current noise passing through the transistors of the ring oscillator, which in the case of a well-balanced perfect ring oscillator is equal for all transistors. It is composed of two components ($i_{th}(\tau)$ and $i_{fl}(\tau)$, which correspond to the impact of the thermal and flicker noises, respectively, indicating their amplitude and their

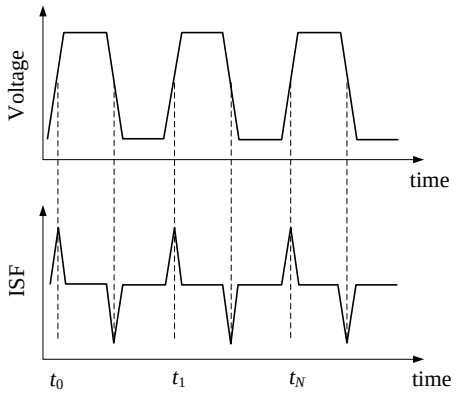

Figure 1: Waveform of the ring oscillator output signal (top) and corresponding Input Sensitivity Function (ISF) (bottom)

behaviour in terms of the power spectral density:

$$\phi(t) = \int_{-\infty}^{t} \frac{\Gamma(\omega_0\tau)}{q_{max}} \cdot i(\tau) \cdot d\tau = \int_{-\infty}^{t} \left(\frac{\Gamma(\omega_0\tau)}{q_{max}} \cdot i_{th}(\tau) + \frac{\Gamma(\omega_0\tau)}{q_{max}} \cdot i_{fl}(\tau) \right) \cdot d\tau. \quad (1)$$

Therefore, the formula describing each period of the ring oscillator measured as a distance between rising (or falling) edges can be reduced to a sum of a product between an amplitude factor and a behavioural factor corresponding to thermal and flicker noises, respectively:

$$dt_i = T_0 + \frac{2\pi}{\omega} \cdot \phi(dt_i) = T_0 + A_{th} \cdot \delta i_{th}(t_i) + A_{fl} \cdot \delta i_{fl}(t_i), \quad (2)$$

where T_0 is the mean period of the ring oscillator, ω is the angular frequency, $\phi(t)$ is the phase at time t, A_{th} and A_{fl} are amplitude factors for the thermal and flicker noise, δi_{th} and δi_{fl} are behavioural terms corresponding to thermal noise and flicker noise. First, it is important to highlight that the last two terms do not necessarily correspond to the amplitudes of the current. The formula indicates that for each period, jitter is determined by an amplitude factor A and a behavioural factor δi. Then, thermal noise depends essentially on the conductance of the transistor channel, whereas flicker noise originates from two mechanisms: carrier number fluctuations coming from the trapping-detrapping of carriers at the interface traps of the gate oxide [MK57] and mobility fluctuations due to scattering in the transistor channel [Hoo69]. Their respective amplitude factors encompass all technological, working and environmental factors determining their amplitude. Furthermore, as the phenomena generating them are different, the two contributions must be considered as independent, hence the lack of a combined term.

The absolute time series is the cumulative sum of the terms described above. Moreover, in case of real measurements, as is the case of TRNGs, the sampling precision is finite. We can therefore transform the integral into a sum:

$$t_i = i \cdot T_0 + \sum_{0}^{t_i} \Big(A_{th} \cdot \delta i_{th}(t_i) + A_{fl} \cdot \delta i_{fl}(t_i) \Big). \quad (3)$$

The following part details the application of the above-mentioned principles in modeling and emulation of the clock jitter behaviour in ring oscillators.

2.2 Model verification using simulations and measurements

Behavioural model. For its general acceptance and universality, the emulator code was developed in Python (available on GitHub[1]). The choice for the Python environment comes from our intention to create an easy-to-use and fast toolbox exploitable by a wide range of developers. Although more sophisticated simulation tools exist, they only provide a more accurate link to technological parameters, without any benefits in terms of behaviour. Besides this, the simulations can prove to be extremely time consuming with no added benefit for TRNG applications. Moreover, phase noise implementation in simulators is hindered by the approximation of the Impulse Sensitivity Function (ISF) which transposes flicker noise into its phase noise contribution. Its determination is complex and the effectiveness of the different methods to cover the entire spectrum of possibilities and regimes does not seem to be a settled question yet [JLH+21].

In order to generate the different noise spectra, we used the "colorednoise" [Pat22] library. Its algorithm is based on an Astronomy and Astrophysics article [TK95] which shows that noise with a certain power spectral signature can be generated by adding multiple random noise contributions with amplitudes corresponding to the desired power spectral density. Due to its simplicity, the results and method are easily verifiable. It should be mentioned that other methods are also available such as the one proposed by Keshner [Kes82] which uses multiple first order filters applied to a random source to generate noise with different power spectral densities. However, as the two methods give similar results, we used the "colorednoise" library for the results presented in this work, due to its easier implementation in the Python script.

Jitter measurements in ASIC. We used the Allan variance to evaluate and compare the jitter parameters in emulator and hardware. The Allan variance is an indicator widely used for TRNG applications [ASP+18] and it is calculated as the variance of the difference between two consecutive samples of the time series corresponding to the rising (or falling) edges of ring oscillator signal. Its behaviour depends on the accumulation time (or the number of the reference clock periods) and varies quadratically (as shown in Fig. 2). The curve begins with a plateau corresponding to the quantization noise which is introduced by the finite resolution of the measurement, followed by a linear region corresponding to the thermal noise and ends with a quadratic part corresponding to the flicker noise. The equation defining those characteristics is: $\sigma_t^2(t) = a_0 + a_1 \cdot t + a_2 \cdot t^2$, where a_0, a_1, a_2 are the factors corresponding to the amplitudes of quantization, thermal and flicker noise, respectively. The fit of the quadratic curve uses the least-squares normalized error (LSNE) regression method [GB06].

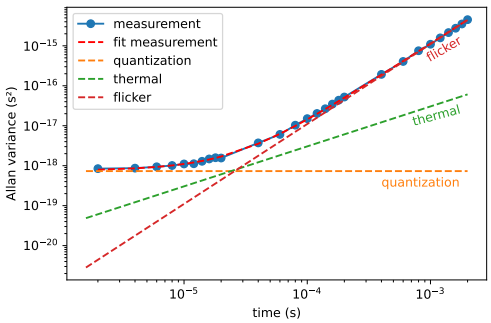

Figure 2: Example of Allan variance characteristics of the jitter obtained from experimental results of RO implemented on a FD-SOI ASIC.

[1] https://github.com/opentrng/papers

In order to isolate as well as possible the physical noise sources, measurements were realized directly on ring oscillators using specific probe station and dedicated equipment. The benefit of this approach is the reduction of other parasitic noise sources by using high precision measurement equipment (analyser and oscilloscope) in an isolated environment (Cascade Elite 300 probe station – specifically conceived to reduce external noise). This methodology enables the characterization of the physical noise source in the most adequate way possible, by reducing the risks associated with cross-talks, noisy voltage sources, less precise embedded measurement and an open environment.

The acquisitions are directly realized on silicon wafers using an up-to date probe station (Cascade Microtech Elite 300). An HP B1500 analyzer imposes the biasing conditions on the DUT (Device Under Test) through SMUs (Source Measurement Units) using a probe card with 25 analog probes with an 80 µm pitch. The output signal of the ring oscillator is recovered through a LAN connection from a Tektronix DPO5104 oscilloscope. All the instrumentation is controlled through a Python program from an external PC (as presented in Fig. 3).

About the impact of the HP B1500 analyzer and the SMU to the noise: as stated in the datasheet, the "force accuracy for the range used (2V) is $0,018\% \pm 400\mu V$". As stated in Fig. 10 in [WJA+14], the sensitivity to VDD variation of a 101 stage RO in a similar FD-SOI technology is roughly about 0,625MHz/mV, that makes 1,28 ps variation in RO period for a $800\mu V$ variation (twice the $400\mu V$), that is roughly 1000 times smaller than the nominal period of the ROs. As stated in Section 3.3, this variation is in the order of magnitude of the jitter measured when quantization noise is dominant (low accumulation times) but but much smaller in the measurement interval, in which the thermal noise and flicker noise contributions dominate. Therefore, the noise contribution of our instrumental set-up is included in the quantization noise and does not alter our model in the thermal and flicker regime.

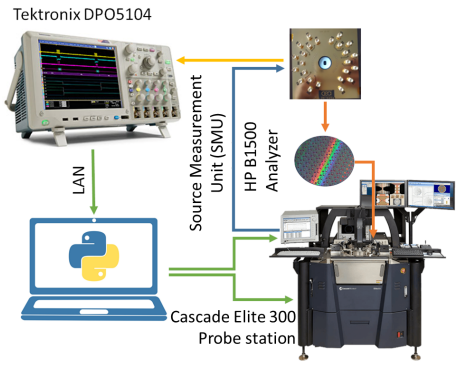

Figure 3: Global view of the measurement chain.

Experimental results are obtained on ring oscillators (RO) fabricated on industrial 28 nm FD-SOI (Fully Depleted Silicon on Insulator) technology. The ROs are composed of 101 inverters, leading to a nominal frequency of 500 MHz. This frequency is typical of those obtained on up-to-date silicon technologies. Measurements are analog (on the rising edge of the RO) and are then processed through an on-chip frequency divider (factor 1024) (schematic in Fig. 4).

The frequency divider makes possible an accurate measurement of the jitter on an oscilloscope. Indeed, we assume that, as we observed in our experiments and as it was published several times in the literature (see for example [HLL99, ASP+18]), jitter is three orders of magnitude smaller than the nominal period. This means that, as the RO has a 2 ns period, jitter would be approximately 2 ps. The oscilloscope used for our measurements (Tektronix DPO5104) has a maximum sample rate of 10GS/s, which

means a sampling step of 100 ps. To the best of our knowledge, none of the commercial oscilloscope have sampling rate above 160 GS/s (sampling step of 6.25 ps). Therefore, none of the commercial oscilloscopes would be able to measure accurately the jitter of our sample. This stresses the importance of the frequency divider. Moreover, frequency dividers are commonly used by the radio-frequency community; their contribution to noise is not frequency dependant and is known to lower noise density by a factor of $20 \cdot log(1/N)$ (where N is factor of division). This can be seen on Fig. 6 presented in [EET11]. The spectral behaviour of the phase noise is only altered by the frequency divider in as to reduce the quantization noise (noise floor) and therefore does not alter our noise measurements.

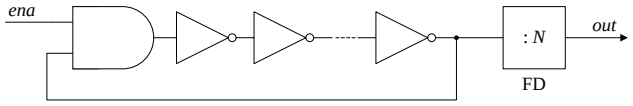

Figure 4: Ring oscillator composed of 101 NOT gates with a frequency divider (FD) before the signal output.

2.3 Model validation by data measured in ASIC

Calibration of the "colorednoise" library to Allan variance. The main goal of the behavioural model is to generate a signal which replicates experimental results (see Fig. 2). More explicitly, the a_0, a_1, a_2 coefficients constitute the input of the emulator, which should generate an equivalent time series corresponding to the emulated ring oscillator periodic signal. As such, the magnification factors between the thermal and the flicker noise generated by the "colorednoise" library and their corresponding Allan variance curves need to be determined first. By generating time series for one unity of thermal and flicker noise (see Eq. (4)), the magnification factors can be directly determined from their corresponding Allan variance. Figure 5 presents the Allan variance results of the unitary times series. The Least Squares Normalized Error Regression [GB06] method is used to estimate $factor_{fl} \approx 0.13$ and $factor_{th} \approx 2$.

$$\begin{cases} dt_i = T_0 + 1 \cdot \delta i_{th}(t_i) + 0 \cdot \delta i_{fl}(t_i) \Rightarrow \sigma_t^2(t) = 0 \cdot t^2 + \text{factor}_{th} \cdot t + 0 \\ dt_i = T_0 + 0 \cdot \delta i_{th}(t_i) + 1 \cdot \delta i_{fl}(t_i) \Rightarrow \sigma_t^2(t) = factor_{fl} \cdot t^2 + 0 \cdot t + 0 \end{cases} \tag{4}$$

Generating emulated data from the behavioural model. Using the a_0, a_1, a_2 parameters obtained by measurement, the relative time series data of the emulator can be computed by developing Eq. (2) into:

$$dt_i = T_0 + \sqrt{\frac{a_1 \cdot T_0}{factor_{th}}} \cdot \delta i_{th}(t_i) + \sqrt{\frac{a_2 \cdot T_0^2}{factor_{fl}}} \cdot \delta i_{fl}(t_i), \tag{5}$$

Where δi_{th}^{RO}, δi_{fl}^{RO} are thermal and flicker noise time series data generated by the "colorednoise" library and T_0 is the nominal period of the ring oscillator. The absolute time series data is obtained by the cumulative sum of the relative time series data. In addition, a quantization effect can be simulated by using the following formula:

$$t_i^{sampled} = q \cdot \lfloor \frac{t_i}{q} + 0.5 \rfloor \tag{6}$$

Where $\lfloor x + 0.5 \rfloor$ is the closest integer of x, and q is the sampling step.

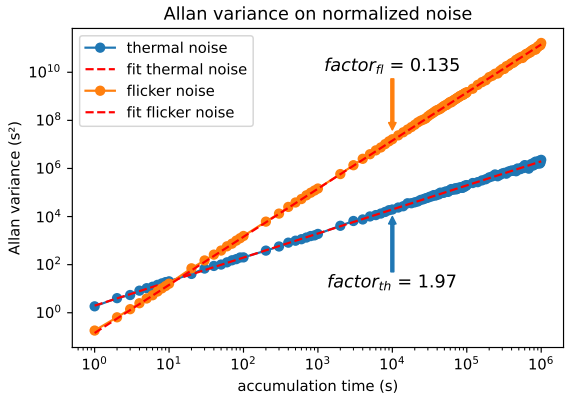

Figure 5: Allan variance of the unitary thermal and flicker noise generated using the colorednoise library in Python.

Figure 6 illustrates the results obtained by calculating the Allan variance of the measured and emulated time series data. The emulated results are closely similar to the results obtained in measurement. Moreover, these results are confirmed by the coefficients of their respective quadratic regression curves, for which the differences are minimal and lower for the quantization noise. However, the emulated quantization noise is in accordance to its theoretical value (see Table 1).

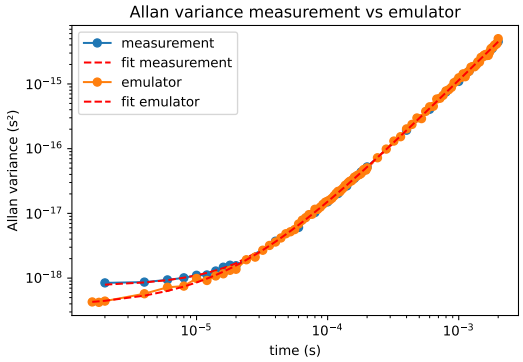

Figure 6: Comparison between measurement and emulator results using the Allan variance. Curve regression realized using the LSNE method.

Table 1: Comparison between the coefficients of the Allan variance obtained by measurement and by emulator in ASIC.

type	$a_2(flicker)$	$a_1(thermal)$	$a_0(quantization)$
Measurement	$1.11.10^{-9}$	$2.56.10^{-14}$	$7.37.10^{-19}$
Emulator	$1.16.10^{-9}$	$2.81.10^{-14}$	$3.23.10^{-19}$
Error	4.75%	9.75%	56.21%

Comparison through histograms. For further verification, the histograms corresponding to the emulated and measured time series for different accumulation times are traced in Fig. 7. Once more, the values generated by the emulator are very similar to those obtained from the real ring oscillator.

Generating data directly for accumulated jitter. Additionally, for an easier implementation of TRNG structures, it is interesting to straightforwardly obtain the time series data corresponding to an accumulation factor N. In order to do so, the period T_0 must be simply modified to $N \cdot T_0$, as given in the following equation:

$$dt_i = N \cdot T_0 + \sqrt{\frac{a_1 \cdot N \cdot T_0}{factor_{th}}} \cdot \delta i_{th}(t_i) + \sqrt{\frac{a_2 \cdot N^2 \cdot T_0^2}{factor_{fl}}} \cdot \delta i_{fl}(t_i) \tag{7}$$

Figure 8 illustrates the histograms obtained from emulated and measured data for different accumulation factors. We can observe that the emulator gives accurate results compared to the ring oscillator's real behaviour. However, we can also observe that the mean value of the measured data slightly deviates for higher accumulation times. This can be explained by the drift of the real ring oscillator. Nonetheless, this deviation is negligible compared to the size of the period.

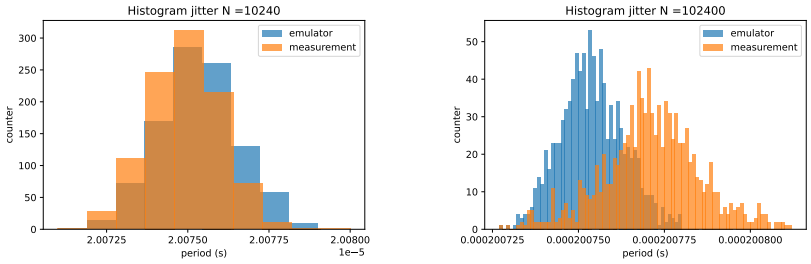

Figure 7: Histogram of the measured and emulated time series data for different accumulation factors: N=20480, N=102400 periods. $T_0 = 2 \cdot 10^{-9}s$, $A_{th} = 6.78 \cdot 10^{-6}s^{-1}$, $A_{fl} = 7.75 \cdot 10^{-9}s^{-1}$.

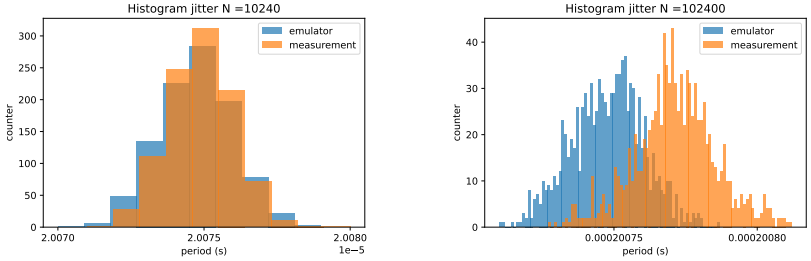

Figure 8: Histograms for measured and emulated time series using directly an accumulation factor of N=10240, N=102400. $T_0 = 2 \cdot 10^{-9}s$, $A_{th} = 6.78 \cdot 10^{-6}s^{-1}$, $A_{fl} = 7.75 \cdot 10^{-9}s^{-1}$.

2.4 Model validation using FPGA

Using the same method, further verifications were realized on FPGA. The measurements were performed on an Arty A7 FPGA development platform manufactured by Digilent. This board embeds a Xilinx Artix 7 100T FPGA, which is built using the TSMC 28nm HPL (High Performance Low Power) foundry process. We implemented our design in the FPGA with two ring oscillators (one used as a source of randomness (RO1) and another one as a reference clock generator(RO0)), a sampling block and a FIFO. The frequencies of the two ROs composing the design are adjustable with a multiplexer used for connecting loopback signals from different stages in the RO back to the input. Each element of the RO is a buffer implemented by an identity function within a LUT5 (five-inputs look-up table) and a NAND gate for loopback, also implemented into a LUT5. We opt for manual placement

over automatic place and route for various reasons. Specifically, we place manually four consecutive buffers within the four LUT5 units of a slice, and we utilize neighbor slices to compose the ring. This approach yields several advantages. Firstly, the results are reproducible after each design compilation. Additionally, with compact RO and shorter routing signals, we diminish phase noise introduced by the nets to the benefit of phase noise introduced by active elements. Lastly, the introduction of empty slices for spacing between the two ROs' slices reduces crosstalk as well as the risk of locking. A data flip-flop (DFF) reads the output of one RO at rising edges of the clock signal generated using the second RO. The DFF output is connected to a FIFO, which can be read from the PC via an UART. In a similar way as in the original article describing the embedded Allan variance computation method [HTBF14], we observe the variations of jitter coming from the ensemble of ring oscillators measured in periods of RO0 for different accumulation factors N of RO0. The Allan variance of the obtained counter values is approximately equal to the normalized jitter with a measurement error which depends on a quantization factor related to the frequency of the clock signal (RO0). As the result is digitized, the formula in Eq. (5) can be adapted for counter values:

$$dN_i = N + \sqrt{\frac{a_1 \cdot N}{factor_{th}}} \cdot \delta i_{th} + \sqrt{\frac{a_2 \cdot N^2}{factor_{fl}}} \cdot \delta i_{fl}, \tag{8}$$

Measurements were realized on a pair of ring oscillators with frequencies $F_{RO1} = 68.20MHz$ and $F_{RO0} = 67.58MHz$. Figure 9 presents a comparison of the measured and generated data in terms of Allan variance (left) and the histogram of the counter values (right) for this configuration. We can observe that the two results are closely matched.

The obtained results for the coefficients corresponding to each noise source are presented in Table 2. First, we observe that the obtained values for flicker noise and thermal noise are close to a precision of some tens of percentages. The inferior precision comes as a result of the poorer sampling on FPGA compared to the precision measurements realized in the previous section.

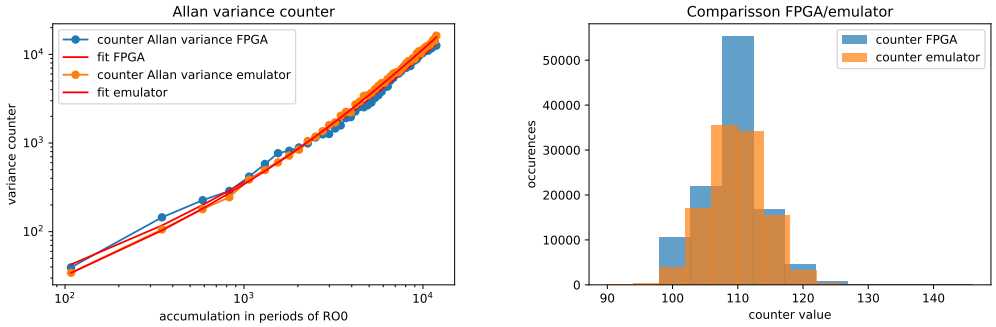

Figure 9: Allan variance (left) and histogram of counter values (right) obtained through FPGA measurement and its respective generated series.

Table 2: Comparison between the coefficients of the Allan variance obtained by measurement and by emulator for FPGA.

		flicker	**thermal**	**quantization**
Device characteristics	counter	$6.90 \cdot 10^{-5}$	$2.81 \cdot 10^{-1}$	$1.15 \cdot 10^{1}$
$F_{RO1} = 68.20MHz$	emulator	$1.02 \cdot 10^{-4}$	$2.35 \cdot 10^{-1}$	$4.47 \cdot 10^{1}$
$F_{RO0} = 67.58MHz$	difference	47.33%	16.29%	61.24%

Hence the reliability of the emulator established, results given by its output will be exploited in the next section to investigate the effect of the thermal and flicker noise on a ring oscillator-based TRNG.

3 Emulation of a complete RO-based TRNG

In this section, we investigate the influence of the thermal and flicker noises on the operating characteristics of a TRNG. The chosen structure is a simplified version of the Elementary Ring Oscillator TRNG (ERO-TRNG). This type of TRNG is used here only as a case study. Other architectures can be tested using the same principle. The architecture was proposed and studied in [BLMT11]. It is made up of two ring oscillators: the first one is used as a generator of a jittered clock signal (source of randomness) and the second one as a generator of the reference clock (which also contains jitter). After the second ring oscillator, a frequency divider is interposed between the ring and the flip-flop so that the jitter accumulated in the first ring during N periods of the second one would be sufficient to generate bits with the required entropy (see Fig. 10).

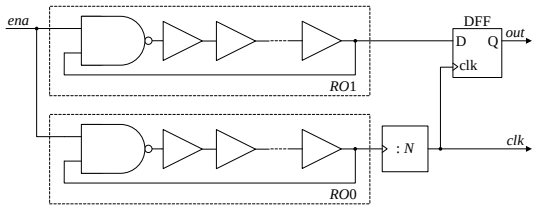

Figure 10: Schematic diagram of an Elementary Ring Oscillator TRNG.

In order to avoid unnecessary confusion and because the main goal of this section is to provide a qualitative study, the emulated ERO-TRNG is composed of only one ring oscillator with jitter (RO0) and a perfect ring oscillator (RO1) in the same way as in [BLMT11]. This represents in fact a mathematical artifice which physically signifies that the jitter of the ensemble of the oscillators is transposed to only one of them. The equations describing the relative time series of the two are:

$$\begin{cases} dt_i^{RO1} = T_0^{RO1} \\ dt_i^{RO0} = T_0^{RO0} + A_{th} \cdot \delta i_{th}^{RO0} + A_{fl} \cdot \delta i_{fl}^{RO0} \end{cases} \tag{9}$$

By recurring to this simplification, the output of such a structure can be calculated by simply calculating the modulus of the absolute time series t_i^{RO0}/T_0^{RO1} with respect to 1. If the result is smaller than the duty cycle, the output bit is 1 and, on the contrary, if the result is greater than the duty cycle, the output bit is 0. If a duty cycle of 50% is considered and if the accumulation factor N of the frequency divider is integrated, the output bit series can be calculated as the closest integer of the modulus of the absolute time series t_i^{RO0}/T_0^{RO1} with respect to 1:

$$\left\lfloor \frac{\sum_{t_i}\left(N \cdot T_0^{RO0} + \sqrt{\frac{a_1 \cdot N \cdot T_0^{RO0}}{factor_{th}}} \cdot \delta i_{th}^{RO0}(t_i) + \sqrt{\frac{a_1 \cdot N^2 \cdot T_0^{RO0\,2}}{factor_{fl}}} \cdot \delta i_{fl}^{RO0}(t_i)\right)}{T_0^{RO1}} mod 1 + 0.5 \right\rfloor \tag{10}$$

This algorithm can be used to generate rapidly the output bits of an ERO-TRNG based on the empirical values a_1, a_2 corresponding to the amplitudes of the thermal and flicker noises. This will enable direct identification of the influences of those two types of noises to the entropy, and the autocorrelation of the TRNG output.

In the followings, we will address the independence of the generated bits by studying the autocorrelation introduced by the flicker noise included in our model.

3.1 Autocorrelation in the generated bit series

The dependencies in a generated bit series can be quantified by the autocorrelation function (ACF). Its coefficients ρ_k of a stationary stochastic process X_n are defined using Pearson's correlation coefficient as:

$$\rho_k = \sum_i \frac{(X_{i+k} - E(X_{i+k}))(X_i - E(X_i))}{\sigma_{X\,i+k}\sigma_{X\,i}} \tag{11}$$

It is important to mention that other functions are also available to determine dependencies such as: (1) the partial autocorrelation function (PACF), which takes into account the effect of the intermediate time steps [BJ76], (2) the autoinformation function (AIF) which analogically to the autocorrelation function uses time-lagged mutual information terms [vWTL17], or (3) the partial autoinformation function (PAIF) which uses conditional mutual information [vW18]. As in our case the results of ACF and AIF were similar and because the PACF and PAIF, by taking into account intermediate terms, have less terms than the former two, the simple autocorrelation function was used in the following analysis.

The autocorrelation of the raw absolute time series (with an accumulation of $N = 100$ periods) was traced in Fig. 11 for different amplitudes of flicker noise. The curve "1*flicker" represents the baseline characteristic of the measured RO implemented in ASIC with the standard amplitudes of thermal and flicker noise. For the other curves, the amplitude of thermal noise remains the same, but the amplitude of flicker noise is proportional to the quantity marked on the legend. We can observe that first, the autocorrelation function increases with the quantity of flicker noise and second, its decline is very slow, as described in [Kes82]. This confirms a long-term influence of previous values, which is indeed disadvantageous for random number generation. This also confirms the validity and the usefulness of our behavioural model.

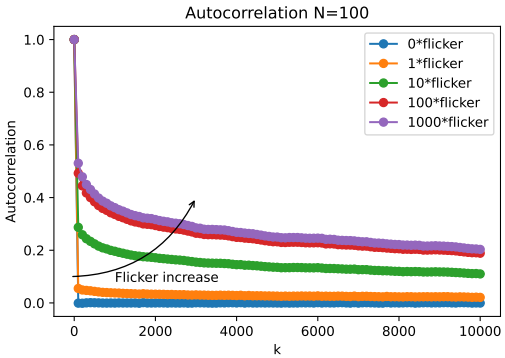

Figure 11: Autocorrelation of the raw absolute time series generated for different amplitudes of flicker noise starting from the baseline of the measured ring oscillator. $T_0 = 2 \cdot 10^{-9}s$, for reference curve (1*flicker):$A_{th} = 6.78 \cdot 10^{-6}s^{-1}$, $A_{fl} = 7.75 \cdot 10^{-9}s^{-1}$.

The autocorrelation function is also calculated for the output bits of the emulated ERO-TRNG for different amplitudes of flicker noise and for different accumulation factors N=100 and N=1000 (see Fig. 12). Surprisingly, in this case, an increase in flicker noise diminishes the depth (in the lag - k axis) and the amplitude of the autocorrelation function. Moreover, the decrease is abrupt and faster when the accumulation factor increases. By

comparison to the raw time series data, we can deduce that the sampling of one of the ring oscillator with the other has an essential effect on the autocorrelation of the generated bits.

In order to test this assumption, the period of RO1 was changed. The autocorrelation function calculated for periods varying from 2 ns to 6 ns was represented in Fig. 13. As a matter of fact, a more stringent sampling reduces the amplitude as well as the depth of the autocorrelation function, proving that the slicing effect caused by the sampling constrains the natural behaviour of flicker noise.

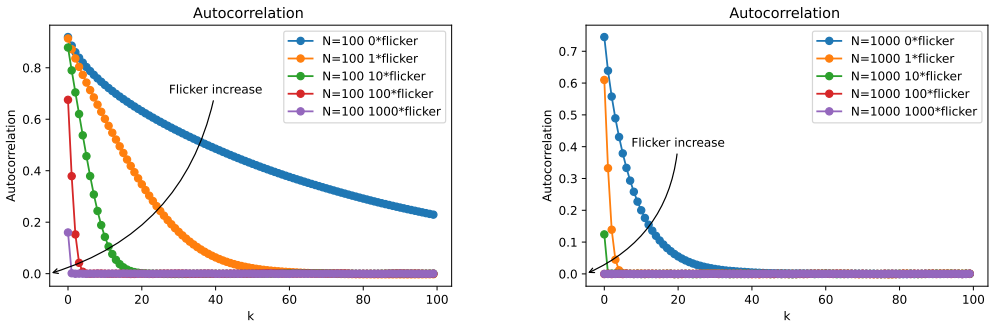

Figure 12: Autocorrelation function calculated on the output bits of the emulated ERO-TRNG for different amplitudes of flicker noise starting from the measured ring oscillator for accumulation factors N=100 (left) and N=1000 (right). $T_0^{RO0} = T_0^{RO1} = 2 \cdot 10^{-9} s$, for reference curve (1*flicker):$A_{th} = 6.78 \cdot 10^{-6} s^{-1}$, $A_{fl} = 7.75 \cdot 10^{-9} s^{-1}$.

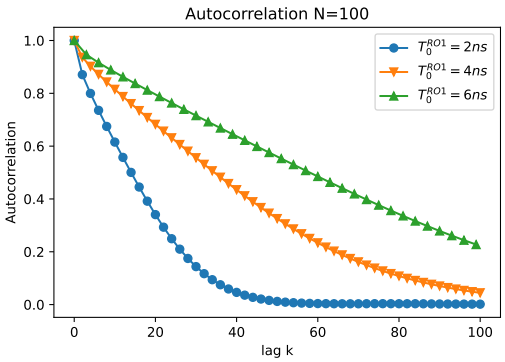

Figure 13: Autocorrelation for different periods of the first ring oscillator. $T_0^{RO0} = 2 \cdot 10^{-9} s$, $A_{th} = 6.78 \cdot 10^{-6} s^{-1}$, $A_{fl} = 7.75 \cdot 10^{-9} s^{-1}$, generated data size 10 000 000 bits.

In order to understand this effect, the absolute jitter of the second ring oscillator (RO0) is traced in Fig. 14 for two different amplitudes of flicker noise: the baseline of the measured ring oscillator on ASIC (1*flicker) and another one with a 10 times larger flicker noise amplitude (10*flicker). The horizontal lines stand for the different domains (slices) corresponding to the output bit of the emulated ERO-TRNG through the closest integer of the modulo operation. One can argue that knowledge of the absolute jitter can straightforwardly determine the output bit. However, from a bit-wise perspective, when a “0” to “1” or a “1” to “0” transition occurs, it is impossible to determine whether it is the result of an increase or a decrease of the absolute jitter. We can observe this effect in Fig. 14 by comparing transitions “1” and “2”. While both are identical in the series of output bits (“1” to “0”), the first one is the result of an increase of the absolute jitter, while the second one is the results of a decrease. One can therefore conclude that the transition

between bits reinitialises the phase reference, making it impossible to guess the trend from previous values. The average memory effect span (the effect of the past on future values) is related to the average time it takes the absolute jitter to switch between domains. This is the reason why a higher flicker noise produces a lower autocorrelation function value, as the absolute jitter is more prone to deviate in the same direction, switching domains more swiftly.

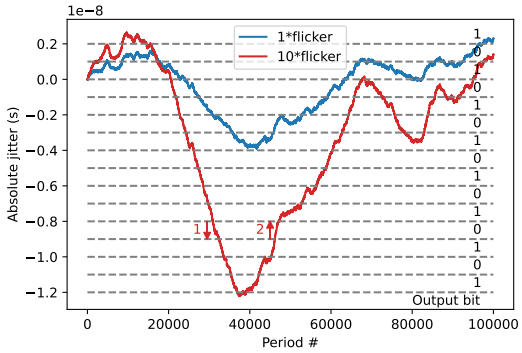

Figure 14: Absolute jitter represented for two time series with different amplitudes of flicker noise. The horizontal lines mark the extent of the different domains corresponding to the output bits of the emulated ERO-TRNG. $T_0 = 2 \cdot 10^{-9}s$, $A_{th} = 6.78 \cdot 10^{-6}s^{-1}$, $A_{fl} = 7.75 \cdot 10^{-9}s^{-1}$.

In order to observe the extent of the autocorrelation function, we define k_0 as the first value of the delay for which the absolute value descends below 0.01. This confidence interval for the absence of correlations was chosen based on the variation of the values close to 0. In analogue 15, the extent of the autocorrelation factor, calculated as $k_0 \cdot N$ (where N is the accumulation factor of the frequency divider), is traced for different accumulation factors and for different amplitudes of flicker noise. Independent of the accumulation factor N of the frequency divider, the extent of ACF remains constant, indicating that the influence of the former values is null beyond a specific point which is constant in time. We conclude that if the frequency divider is set to a value greater than the extent of the autocorrelation, the autocorrelation of the output bits is null. Moreover, as observed from Fig. 12, the depth of the autocorrelation function decreases with the amplitude of the flicker noise.

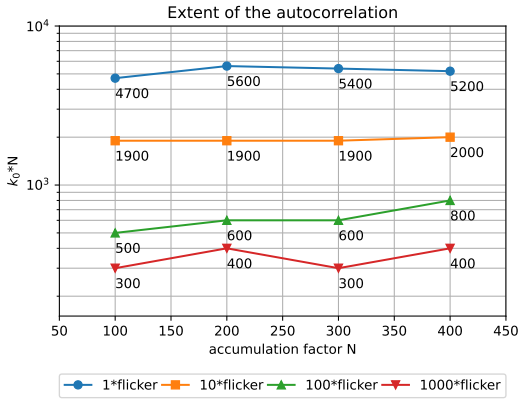

Figure 15: The extent of the autocorrelation function for different accumulation factors and for different amplitudes of flicker noise. Results obtained using the same methodology as for the results presented in Fig. 12.

As stated previously, the extent of the autocorrelation function is related to the average time it takes absolute jitter to switch between domains. However, the average of the squared deviation is given by the Allan variance, and its dependence in time is given by the accumulation time. Therefore, for a domain size ($\frac{T_0^{RO1}}{2}$) equivalent to a particular value of the Allan variance, the depth of the autocorrelation function can be obtained by determining the accumulation time corresponding to that particular Allan variance value. In Fig. 16, the depth of the autocorrelation function for different sizes of domains equal to $T_0^{RO1} = \{1, 2, 4, 10, 20, 40, 100\} \times 2ns$ was traced as $k_0 \cdot N$. On the x-axis, the depth is bound by the Allan variance curve and is slightly lower. This underestimation can be explained by the fact that k_0 is determined at a 0.01 value of the ACF. If a lower value would be achieved in practice, the results would be closer.

In order to obtain an analytical solution for the depth in time of the autocorrelation function, one needs to solve the quadratic equation coming from the equivalence between the Allan variance of RO0 and the size of the domain (half of the period of the first ring oscillator) squared. Note that only the positive solution makes physical sense and is developed in Eq. (12).

$$a_2 \cdot t^2 + a_1 \cdot t = \left(T_0^{RO1}/2\right)^2 \Rightarrow t = \frac{-a_1 + \sqrt{a_1^2 - 2 \cdot a_2 \cdot {T_0^{RO1}}^2}}{2 \cdot a_2} \tag{12}$$

In order to convert the solution in number of periods of the second ring oscillator, the result must be divided by T_0^{RO1}. The values obtained from the two methods are presented in Table 3. As observed in Fig. 16, the results obtained using the Allan variance are always greater than the ones obtained by the graphical period due to the confidence interval needed to determine k_0.

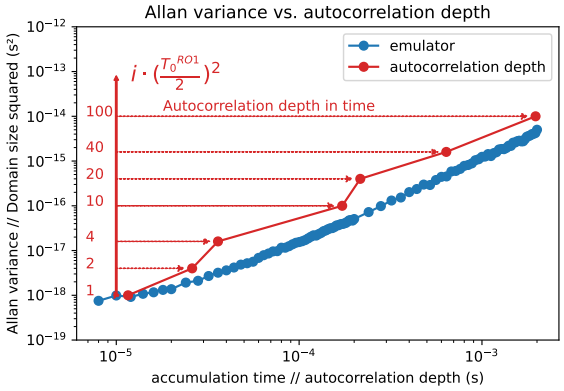

Figure 16: Comparison between the Allan variance and the depth in time of the Autocorrelation function. $T_0^{RO0} = T_0^{RO1} = 2 \cdot 10^{-9}s, A_{th} = 6.78 \cdot 10^{-6}s^{-1}, A_{fl} = 7.75 \cdot 10^{-9}s^{-1}$.

Table 3: Extent of the autocorrelation function calculated using the graphical method and the Allan variance.

Size of T_0^{RO1}	**ACF extent as $(N \cdot k_0)$**	**ACF extent from Allan variance**	**Difference (%)**
$T_0^{RO1} = 2ns$	5800	9870	70.17%
$2 \cdot T_0^{RO1}$	13000	23604	81.57%
$4 \cdot T_0^{RO1}$	18000	51757	187.54%
$10 \cdot T_0^{RO1}$	86000	136793	59.06%
$20 \cdot T_0^{RO1}$	108000	278716	158.07%
$40 \cdot T_0^{RO1}$	319000	562634	76.37%
$100 \cdot T_0^{RO1}$	982000	1414448	44.04%

The obtained results allow us to conclude that the dependence of the generated bits introduced by the flicker noise is finite. After the accumulation point corresponding to the equivalence between the Allan variance and the squared half-period of RO1, the generated bits can be considered as independent. We recall that the flicker noise is considered non-stationary because of its divergence when the frequency tends to 0. However, the previously presented results show that there is a lower frequency boundary, which comes as a result of sampling a clock signal using another clock signal. The jitter accumulation during the time interval t can be broken into different time intervals corresponding to transitions between domains synonymous to a "0" and "1" output of the generator. The integration between transitions modulo 1 is always null because the deviations are equal to the period ($T_0/T_0 \bmod 1 = 0$). Therefore, the generated bit at time t is only dependant on the integration over the last domain, cancelling all previous contributions and thus any memory effect. If the accumulation time of jitter is greater than the time between transitions, the only way to predict the output of the generator would be to precisely measure the jitter in real time, which is technically implausible. In the following section, we will investigate the influence of the flicker noise on entropy and its implication on the principle and performance of the TRNG.

3.2 Influence of the flicker noise on the entropy

Assuming independence, the entropy calculated on blocks of n bits can be determined using the following formula:

$$H_n = \sum_{b \in (0,1)^n} p(b) \cdot log(p(b)) \tag{13}$$

Where p_i describes the probability of an n-bit pattern. We will use the entropy of blocks of n bits as an indicator used to quantify the influence of thermal and flicker noises on the entropy. We admit that Eq. (13) is valid only under an independence condition, which is our case is described by a null autocorrelation. Therefore, we will use this indicator as a mean of comparing results obtained from series which differ only in terms of the amplitudes of thermal or flicker noise.

First, the size of the n-bit pattern which enables a good approximation of entropy needs to be determined. Figure 17 illustrates the entropy H_n calculated for different n: 2, 4, 6, 8, 16. For a better comparison, the results were normalized by dividing the entropy by n, so that the results represent H_n/n. We observe that the results converge for high n. therefore, we assume that this measure can be a good approximation for the entropy rate. For the following results an 8-bit pattern will be used.

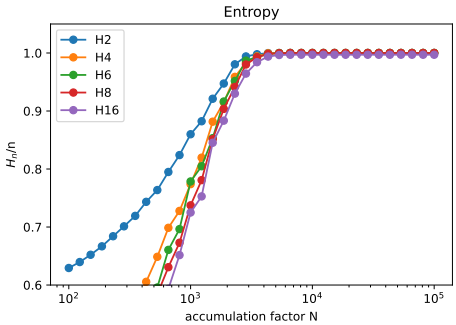

Figure 17: Entropy calculated for different sizes of the n-bit pattern: 2, 4, 6, 8, 16 bits. $T_0^{RO0} = T_0^{RO1} = 2 \cdot 10^{-9}s$, $A_{th} = 6.78 \cdot 10^{-6}s^{-1}$, $A_{fl} = 7.75 \cdot 10^{-9}s^{-1}$, generated data size 1 000 000 bits.

Figure 18 shows the entropy dependence on the accumulation time (division factor N of the frequency divider), for different configurations of thermal noise (left) and flicker noise (right). The baseline characteristics (H8) of the emulator correspond to an emulated RO0 with characteristics similar to the ones of the ring oscillator implemented in ASIC presented in Section 2. The amplitudes of the injected noises vary in a logarithmic scale from 0 to 100 times the amount of the measured noise. On the left panel of Fig. 18, thermal noise amplitude remains constant and flicker noise amplitude is proportional to the quantity marked on the legend. On the right panel of Fig. 18, flicker noise remains constant and thermal noise amplitude varies. The obtained values are also benchmarked against the existing model [BLMT11] which uses only the thermal component of jitter to determine the minimal entropy. The results show that higher thermal and flicker noise have a positive influence on entropy. Moreover, as expected, the existing model represents a lower boundary of the entropy rate compared to the values obtained directly from the output bits. Furthermore, the curve corresponding to thermal noise only (left panel in Fig. 18 in green ▼) is closely approaching the one obtained using Baudet *et al.* model. This confirms the choice of the 8-bit approximation and the validity of our behavioural model.

In the upper part of Fig. 18, the accumulation points corresponding to a null autocorrelation of the bit series are represented on each curve above the line "ACF=0". Those points were determined using the Allan variance method. They all appear for entropy rates greater than 0.997 and could constitute the operating points in terms of jitter accumulation necessary for TRNG operation. The corresponding theoretical output of the generator for different quantities of integrated flicker noise is represented in Fig. 19. We can observe that by integrating the flicker noise in the stochastic model, the TRNG performance can be significantly increased. For the existing model [BLMT11], which neglects the contribution of flicker noise, the output bit rate would be 307 kbits/s. By including a realistic amount of the flicker noise, the output bit rate of the generator would increase four fold to 1.27Mbits/s. This motivates and confirms the necessity of integrating flicker noise as a valuable noise source. If the proportion of the flicker noise in the total noise level would further increase (as could be expected in future technologies), the output bit rate could increase even more.

4 Conclusions

We proposed simple and reliable behavioural model designed to simulate behaviour of ring oscillator-based TRNG architectures. We have shown that the emulator output corresponds well to timings in the real ring oscillators and that it accurately replicates real measurements. Based on this, we realized a simple version of the RO-TRNG, enabling to study contributions of the thermal and flicker noises on the operating characteristics of the generator. The performances of ring oscillator-based TRNGs are often hindered by neglecting the flicker noise as a source of entropy because of its autocorrelated behaviour, expected to cause predictability of the generated bits. The results presented in this paper show that the sampling of the jittered clock signal on the rising edges of another clock signal coming from a different ring conceals the autocorrelation effect induced by the flicker noise. This reduces the predictability to an extent which corresponds to the average time it takes the absolute jitter to switch between domains corresponding to a half of the sampled period of the sampled ring oscillator. Ultimately, the flicker noise can be considered as an additional contributor to the output entropy rate if the accumulation factor is larger than the extent of the autocorrelation in the bit series. This can significantly increase the output bit rate while maintaining the targeted entropy rate of the TRNG by permitting lower accumulation times. Our future work will be dedicated to building a stochastic model which would assimilate the flicker noise in entropy estimation. Such a model should include technological parameters at the transistor level.

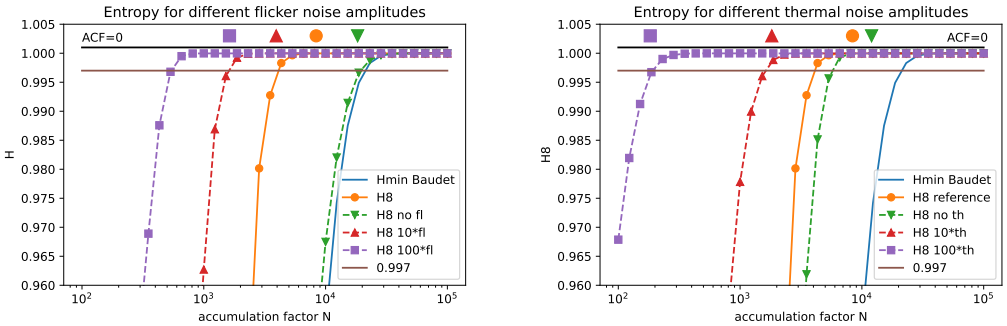

Figure 18: Entropy calculated on the emulated ERO-TRNG with different amplitudes of thermal noise (left) and of flicker noise (right).). $T_0^{RO0} = T_0^{RO1} = 2 \cdot 10^{-9} s$, for reference curve (H8):$A_{th} = 6.78 \cdot 10^{-6} s^{-1}$, $A_{fl} = 7.75 \cdot 10^{-9} s^{-1}$, generated data size 1 000 000 bits.

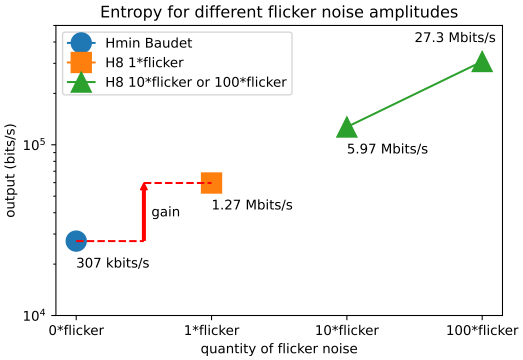

Figure 19: Expected output bit rate of the ERO-TRNG depending on the quantity of the flicker noise computed for the Shannon entropy rate 0.997 per bit. '1*flicker' is the reference quantity of the measured RO in section 2.3. '10*flicker' and '100*flicker' induce a 10, respectively 100, times larger amplitude of flicker noise.

5 Acknowledgements

This work is supported by the "France 2030" government investment plan managed by the French National Research Agency (ANR), under the project ARSENE (ANR-22-PECY-0004).

References

[AATS17] Antonio J. Acosta, Tommaso Addabbo, and Erica Tena-Sánchez. Embedded electronic circuits for cryptography, hardware security and true random number generation: an overview: EMBEDDED ELECTRONIC CIRCUITS FOR CRYPTOGRAPHY. *International Journal of Circuit Theory and Applications*, 45(2):145–169, February 2017.

[Abi06] A.A. Abidi. Phase Noise and Jitter in CMOS Ring Oscillators. *IEEE Journal of Solid-State Circuits*, 41(8):1803–1816, August 2006.

[All66] D.W. Allan. Statistics of atomic frequency standards. *Proceedings of the IEEE*, 54(2):221–230, 1966.

[ASP+18] Elie Noumon Allini, Maciej Skórski, Oto Petura, Florent Bernard, Marek Laban, and Viktor Fischer. Evaluation and monitoring of free running oscillators serving as source of randomness. *IACR TCHES*, 2018(3):214–242, 2018. https://tches.iacr.org/index.php/TCHES/article/view/7274.

[BCPPW22] L. Benea, M. Carmona, F. Pebay-Peyroula, and R. Wacquez. On the Characterization of Jitter in Ring Oscillators using Allan variance for True Random Number Generator Applications. In *2022 25th Euromicro Conference on Digital System Design (DSD)*, pages 534–538, Maspalomas, Spain, August 2022. IEEE.

[BJ76] George EP Box and Gwilym M. Jenkins. Time series analysis: Forecasting and control San Francisco. *Calif: Holden-Day*, 1976.

[BLMT11] Mathieu Baudet, David Lubicz, Julien Micolod, and André Tassiaux. On the security of oscillator-based random number generators. *Journal of Cryptology*, 24(2):398–425, April 2011.

[EET11] EETimes. EETimes - Perfect timing: performing clock division with jitter and phase noise measurements, August 2011.

[FL14] Viktor Fischer and David Lubicz. Embedded evaluation of randomness in oscillator based elementary TRNG. In Lejla Batina and Matthew Robshaw, editors, *CHES 2014*, volume 8731 of *LNCS*, pages 527–543. Springer, Heidelberg, September 2014.

[GB06] B.E. Grantham and M.A. Bailey. A Least-Squares Normalized Error Regression Algorithm with Application to the Allan Variance Noise Analysis Method. In *2006 IEEE/ION Position, Location, And Navigation Symposium*, pages 750–756, Coronado, CA, 2006. IEEE.

[GRND+91] G. Ghibaudo, O. Roux, Ch. Nguyen-Duc, F. Balestra, and J. Brini. Improved Analysis of Low Frequency Noise in Field-Effect MOS Transistors. *physica status solidi (a)*, 124(2):571–581, 1991. _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/pssa.2211240225.

[HFBN15] Patrick Haddad, Viktor Fischer, Florent Bernard, and Jean Nicolai. A physical approach for stochastic modeling of TERO-based TRNG. In Tim Güneysu and Helena Handschuh, editors, *CHES 2015*, volume 9293 of *LNCS*, pages 357–372. Springer, Heidelberg, September 2015.

[HLL99] A. Hajimiri, S. Limotyrakis, and T.H. Lee. Jitter and phase noise in ring oscillators. *IEEE Journal of Solid-State Circuits*, 34(6):790–804, June 1999.

[Hoo69] Friits N. Hooge. 1/f noise is no surface effect. *Physics letters A*, 29(3):139–140, 1969. Publisher: Elsevier.

[HTBF14] Patrick Haddad, Yannick Teglia, Florent Bernard, and Viktor Fischer. On the assumption of mutual independence of jitter realizations in P-TRNG stochastic models. In *Design, Automation & Test in Europe Conference & Exhibition (DATE), 2014*, pages 1–6, Dresden, Germany, 2014. IEEE Conference Publications.

[JLH+21] Zirui Jin, Dongsheng Liu, Ang Hu, Xiaoyu Shan, Chengcheng Zhang, Yanwen Su, Xuecheng Zou, and Xu Zhao. An accurate isf-based analysis and simulation method for phase noise in lc/ring oscillators. *Microelectronics Journal*, 117:105240, 2021.

[Kes82] Marvin S. Keshner. 1/f noise. *Proceedings of the IEEE*, 70(3):212–218, 1982. Publisher: IEEE.

[KG04] Paul Kohlbrenner and Kris Gaj. An embedded true random number generator for FPGAs. In *Proceeding of the 2004 ACM/SIGDA 12th international symposium on Field programmable gate arrays - FPGA '04*, page 71, Monterey, California, USA, 2004. ACM Press.

[KS11] Wolfgang Killmann and Werner Schindler. A proposal for: Functionality classes for random number generators, version 2.00. [online] Available at https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_31_Functionality_classes_for_random_number_generators_e.pdf?__blob=publicationFile, 2011.

[MK57] A. L. McWhorter and R. H. Kingston. Semiconductor surface physics. *University of Pennsylvania, Philadelphia*, 207, 1957.

[Pat22] Felix Patzelt. Colorednoise, April 2022.

[SMS07] Berk Sunar, William Martin, and Douglas Stinson. A Provably Secure True Random Number Generator with Built-In Tolerance to Active Attacks. *IEEE Transactions on Computers*, 56(1):109–119, January 2007.

[TBK+18] Meltem Sönmez Turan, Elaine Barker, John Kelsey, Kerry A McKay, Mary L Baish, and Mike Boyle. Recommendation for the entropy sources used for random bit generation. Technical Report NIST SP 800-90b, National Institute of Standards and Technology, Gaithersburg, MD, January 2018.

[TK95] Jens Timmer and Michel Koenig. On generating power law noise. *Astronomy and Astrophysics*, 300:707, 1995.

[VD10] Michal Varchola and Milos Drutarovsky. New high entropy element for FPGA based true random number generators. In Stefan Mangard and François-Xavier Standaert, editors, *CHES 2010*, volume 6225 of *LNCS*, pages 351–365. Springer, Heidelberg, August 2010.

[vW18] Frederic von Wegner. Partial Autoinformation to Characterize Symbolic Sequences. *Frontiers in Physiology*, 9:1382, October 2018.

[vWTL17] F. von Wegner, E. Tagliazucchi, and H. Laufs. Information-theoretical analysis of resting state EEG microstate sequences - non-Markovianity, non-stationarity and periodicities. *NeuroImage*, 158:99–111, September 2017.

[WJA+14] O. Weber, E. Josse, F. Andrieu, A. Cros, E. Richard, P. Perreau, E. Baylac, N. Degors, C. Gallon, E. Perrin, S. Chhun, E. Petitprez, S. Delmedico, J. Simon, G. Druais, S. Lasserre, J. Mazurier, N. Guillot, E. Bernard, R. Bianchini, L. Parmigiani, X. Gerard, C. Pribat, O. Gourhant, F. Abbate, C. Gaumer, V. Beugin, P. Gouraud, P. Maury, S. Lagrasta, D. Barge, N. Loubet, R. Beneyton, D. Benoit, S. Zoll, J.-D. Chapon, L. Babaud, M. Bidaud, M. Gregoire, C. Monget, B. Le-Gratiet, P. Brun, M. Mellier, A. Pofelski, L.R. Clement, R. Bingert, S. Puget, J.-F. Kruck, D. Hoguet, P. Scheer, T. Poiroux, J.-P. Manceau, M. Rafik, D. Rideau, M.-A. Jaud, J. Lacord, F. Monsieur, L. Grenouillet, M. Vinet, Q. Liu, B. Doris, M. Celik, S.P. Fetterolf, O. Faynot, and M. Haond. 14nm FDSOI technology for high speed and energy efficient applications. In *2014 Symposium on VLSI Technology (VLSI-Technology): Digest of Technical Papers*, pages 1–2, June 2014. ISSN: 2158-9682.