On the assumption of mutual independence of jitter realizations in P-TRNG stochastic models

Patrick Haddad, Yannick Teglia, Florent Bernard, Viktor Fischer

On the assumption of mutual independence of jitter realizations in P-TRNG stochastic models

Patrick Haddad, Yannick Teglia
STMicroelectronics
Advanced System Technology
Av. Coq, 13790 Rousset , France
Email: (patrick.haddad, yannick.teglia)
@st.com

Florent Bernard, Viktor Fischer
Hubert Curien Laboratory
UMR CNRS 5516, Jean Monnet University
18 rue Prof. Lauras, St.-Etienne, France
Email: (florent.bernard,fischer)
@univ-st-etienne.fr

***Abstract*—Security in true random number generation in cryptography is based on entropy per bit at the generator output. The entropy is evaluated using stochastic models. Several recent works propose stochastic models based on assumptions related to selected physical analog phenomena such as noise or jittery signal and on the knowledge of the principle of randomness extraction from the obtained analog signal. However, these assumptions simplify often considerably the underlying analog processes, which include several noise sources. In this paper, we present a new comprehensive multilevel approach, which enables to build the stochastic model based on detailed analysis of noise sources starting at transistor level and on conversion of the noise to the clock jitter exploited at the generator level. Using this approach, we can estimate proportion of the jitter coming only from the thermal noise, which is included in the total clock jitter.**

I. Introduction

Random number generation is a critical issue in numerous cryptographic applications: it is used for generation of initialization vectors, challenges, nonces and confidential keys. A flaw in security of the random number generation impacts directly the security of the whole cryptographic system. Random number generators are classified into two main categories: deterministic random number generators (or deterministic random bit generators) and physical true random number generators (P-TRNG). While the deterministic generators are based on algorithmic processes, the P-TRNGs exploit noisy analog phenomena in electronic devices to produce random bit streams. The vulnerability of the P-TRNG to non-invasive attacks has been recently highlighted in [3] and [4]. Thus, designers should take into account such vulnerabilities in order to increase the robustness of the generators against attacks. Currently, the security assessment of the P-TRNG is based on both robustness of the source of entropy and on on-line execution of simple tests of the source of randomness, which are adapted to the structure of the generator. Concerning the first security objective (robustness), the generator principle must ensure that the randomness in the generated sequence is due to the desired noisy physical phenomenon that is not manipulated. Concerning the second security objective (detection of attacks), the dedicated tests are based on a design specific stochastic model, which describes the behavior of the generator. Several recent articles such as [5],[6],[7],[8] and [9] proposed such descriptions. Most of these models are based on assumptions that are difficult or impossible to validate. In this paper we propose to refine existing models by taking into consideration the electronic randomness sources at transistor level. Such a refinement will allow us to show that assumptions of existing models can be considered to be incomplete.

The paper is organized as follows: in Section 2 we analyse existing P-TRNG stochastic descriptions and we position our contribution in the state of the art. Our contribution is presented in details in Sections 3 and 4. We conclude the paper by a discussion concerning the impact of presented results on existing P-TRNG stochastic models.

978-3-9815370-2-4/DATE14/©2014 EDAA

II. Analysis of existing P-TRNG stochastic models

A. Characteristics of a P-TRNG according to AIS31

According to AIS 31 [10], a P-TRNG is composed of three entities as depicted in Fig 1.

- The entropy source is the core of the P-TRNG, it is defined as the electronic circuit generating a raw random analog signal (RRAS).
- The digitizer transforms this analog signal into a raw binary sequence.
- The post-processing block executes a determinist algorithm. This algorithm may be applied to the raw binary sequence in order to increase its entropy per bit (algebraic post-processing) and/or to increase security (cryptographic post-processing).

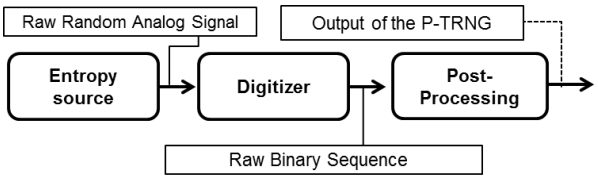

Fig. 1. P-TRNG according to AIS31

The choice of the entropy source and of the digitizer can change from one P-TRNG to another. However, almost all P-TRNGs implemented in logic devices exploit random variations of delays in logic gates.

B. Analysis of existing P-TRNG stochastic descriptions

Recent works ([5],[6],[7],[8] and [9]) proposed stochastic descriptions of the raw binary sequence generated by different kinds of P-TRNG. In [5], Bernard et al. proposed a model of the raw binary sequence generated by a PLL-based P-TRNG. A similar work was performed by Amaki in [6] and Baudet in [8] in case of P-TRNG based on classical ring oscillators. In these two cases, the authors describe first the behavior of the RRAS (model of the entropy source). This description is based on assumptions on the RRAS and take as an input at least one parameter representing the jitter distribution. This description is then combined with a model of the digitization process in order to provide a stochastic description of the raw binary sequence. This description allows to determine the theoretical value of the entropy per bit before the post-processing. The above described approach is depicted in Fig. 2.

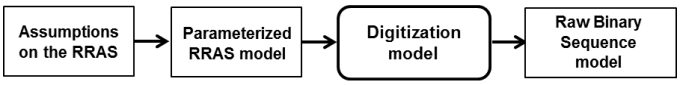

Fig. 2. Common approach in P-TRNG stochastic descriptions

During our experiments and study of entropy sources, we found out that assumptions (e.g. independence of jitter realizations) that were used in most of TRNG stochastic models did not correspond to the reality and that they needed some important adjustments. The precision of models is very important for good entropy estimation and thus for security evaluation of the TRNG.

C. Our contribution to the state of the art

Our contribution consists in refining the existing approaches in TRNG stochastic modeling. We propose to replace the assumptions on the raw random analog signal by a model obtained following a careful study of physical analog phenomena (i.e. the entropy source) at transistor level. This proposal, denoted as the multilevel approach, is presented in Fig. 3.

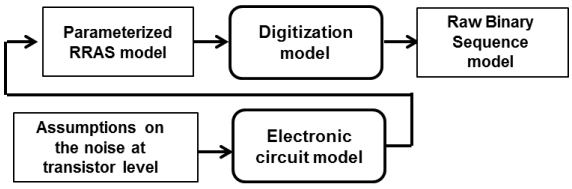

Fig. 3. Proposed multilevel randomness harvesting model approach

In our approach, we replace the difficulty of verifying high level assumptions by stronger and well validated low level assumptions based on semiconductor physics, which are used to characterize electronic noises (i.e. the sources of entropy). In particular, we pay attention to the process which transforms these noises at transistor level into RRAS. The analysis of this process combined with the theory of the noise generation at transistor level allows us to describe more precisely the behavior of the RRAS signal. Most P-TRNGs, which are modeled in the state of the art, exploit the delay variation of logic gates (i.e. the jitter). In order to evaluate the commonly used approach from Fig. 2, we will study the origin of the jittery clock behavior and its impact on the RRAS, when this clock is generated by a classical ring oscillator (depicted in Fig. 4) used as the entropy source.

III. Analysis of the RRAS in rings oscillators

Numerous P-TRNGs based on classical ring oscillators have already been published in the literature. Some recent works [6], [8] focused on the proposal of a stochastic description of the raw binary sequence generated by a simple P-TRNG based on classical ring oscillators – a kind of elementary ring oscillator based TRNG (eRO-TRNG). The eRO-TRNG is depicted in Fig. 4.

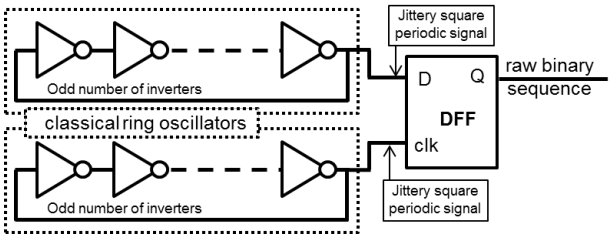

Fig. 4. Elementary RO-TRNG based on classical ring oscillators

The eRO-TRNG is made of two classical ROs. The RRAS is assumed to be the relative jitter between the two ring oscillators. This jitter represents basically the relative noise of the two oscillator periods. In state of the art approaches, the relative jitter is considered to be a random process with independent realizations. Next, we will verify the validity of this assumption by studying the relationship between the jitter and the electronic noise at transistor level.

A. Parasitic quantum phenomena at transistor level

Several quantum phenomena impact the normal behavior of a transistor. Their impact is usually modeled by an additional current source between the drain and the source (noted i_{ds}). The noise current generated by these phenomena is characterized by its power spectral density (PSD). In [11] Lundberg described most of these phenomena. In particular, he noted that the noise behavior of bulk CMOS devices is dominated primarily by two noise sources: the thermal noise, which is a non-auto correlated noise, and the flicker noise, which is an autocorrelated noise. In this paper, we will consider the impact of these two types of noise at transistor level on the clock jitter.

The thermal noise current PSD is given as [12]:

$$S_{i_{ds}th}(f) = \frac{8}{3} \cdot T \cdot k \cdot g_m$$

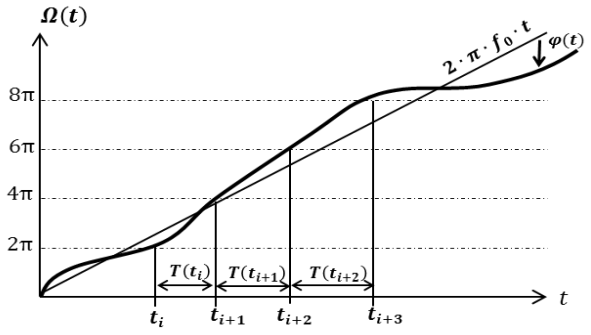

Fig. 5. T and consecutive rising edges of the oscillator

Where k is the Boltzmann constant, T is the temperature, and g_m is the transconductance of the transistor.

The flicker noise current PSD is given as follows [13]:

$$S_{i_{ds}fl}(f) = \alpha \cdot \frac{T \cdot k \cdot {I^2}_D}{W \cdot L^2 \cdot f}$$

Where f is the Fourier frequency of the noise, α is a constant associated to the crystallography of the silicon, L is the channel length of the transistor, W is its section and I_D is the nominal current between the drain and the source.

Because parasitic phenomena related to these two noise current sources are independent, we can say that the PSD of i_{ds} is:

$$S_{i_{ds}}(f) = S_{i_{ds}th}(f) + S_{i_{ds}fl}(f) \tag{1}$$

We will analyze the process, which converts i_{ds} into the jitter. In particular, we will study how the two noise sources impact the independence of jitter realizations.

B. Definitions and properties

1) Definition:

Let us consider an oscillating signal generated by a classical ring oscillator. Let us describe this signal as follows:

$$V_{out}(t) = P[\Omega(t)] \tag{2}$$

with:

$$\Omega(t) = 2 \cdot \pi \cdot f_0 \cdot t + \phi(t)$$

Where P is a 2π-periodic square function, f_0 is the nominal frequency of the ring oscillator and $\phi(t)$ is the excess phase caused by electronic noises.

Let $T = (T(t_i))_i$ be a random process discrete in time (also known as a time series), which describes the time difference between two consecutive rising edges of the oscillator (depicted in Fig. 5) and let $J = (J(t_i)_i)$ be the random process representing the period jitter of the signal. J is defined in relation to T by:

$$J = T - \frac{1}{f_0} \tag{3}$$

Now, we will study the impact of i_{ds} on J and especially on the independence of its realizations.

2) Properties due to the independence of jitter realizations:

According to Bienaymé's formula, the variance of the sum of uncorrelated random variables equals the sum of their variances.

If random variables $J(t_i)$ are mutually independent, they are uncorrelated and the Bienaymé's formula holds for $(J(t_i)_i)$

$$\text{Var}\left(\sum_{i=1}^{n} J(t_i)\right) = \sum_{i=1}^{n} \text{Var}(J(t_i))$$

As a consequence, the contra-position of this proposition says that if Bienaymé's formula is wrong, then the random variables $(J(t_i))_i$ are not independent.

It is the reason why in order to evaluate independence of jitter realizations, it is important to analyze the sum of variances of jitter realizations. However in [2] Allan showed that due to noises that are inversely proportional to the frequency (e.g. flicker noise), the variance of the jitter can not be theoretically calculated. Instead, Allan proposed to compute a 2-sample variance [1].

Following the same ideas as Allan, we focus on a random process representing the difference of two accumulations of the same number of periods and compute its variance, which is possible even in the presence of the flicker noise.

For this reason, we study the random process $(s_N(t_i))_i$, whose realizations are defined as follows:

$$s_N(t_i) = \sum_{j=0}^{2 \cdot N-1} a_j \cdot J(t_{i+j}) \tag{4}$$

where

$$a_j = \begin{cases} -1 & \text{if} \quad 0 \leq j \leq N-1 \\ 1 & \text{else} \end{cases}$$

Let σ_N^2 be the variance of s_N. If we assume that the random variable $J(t_i)$ is approximated by

$$J(t_i) = \frac{\phi(t_i) - \phi(t_i + \frac{1}{f_0})}{2 \cdot \pi \cdot f_0} \tag{5}$$

then

$$\sigma_N^2 = \frac{2}{f_0^2} \cdot \sigma_y^2\left(\frac{N}{f_0}\right)$$

where σ_y^2 is the Allan variance[1].

However, because this expression is based on the above mentioned approximation (5), which depends on the process that we wish to fairly characterize (ϕ), we decided to use another way of evaluating the variance. Using the Bienaymé formula in (4) we can say that if $\{J(t_k)\}_{k=i\cdots i+2N-1}$ are $2N$ mutually independent realizations:

$$\sigma_N^2 = \sum_{j=0}^{2 \cdot N-1} a_j^2 \cdot Var(J(t_{i+j}))$$

Moreover, because the jitter is a stationary process, its variance is σ^2: $\forall j \in \{0 \cdots 2N-1\}$, $Var(J(t_{i+j})) = \sigma^2$. Consequently:

$$\sigma_N^2 = 2 \cdot N \cdot \sigma^2 \tag{6}$$

We can conclude that if $2N$ consecutive jitter realizations are mutually independent, the accumulated variance is a linear function of N, given by (6).

We will use this property in order to study the independence of jitter realizations. Moreover, by establishing the link between noise currents and σ_N^2 we will also understand how they impact the independence of jitter realizations.

C. From noise currents to σ_N^2

Let t_i and t_{i+1} be two consecutive rising edges of the oscillator, and like [14] let us write $T(t_i)$: the realization of T between t_i and t_{i+1} using:

$$T(t_i) = \frac{1}{f_0} + \frac{\phi(t_i) - \phi(t_{i+1})}{2 \cdot \pi \cdot f_0} \tag{7}$$

By using (7) and (3) in (4), we can write s_N as follows:

$$s_N(t_i) = -\frac{\phi(t_{i+2N}) - 2 \cdot \phi(t_{i+N}) + \phi(t_i)}{2 \cdot \pi \cdot f_0} \tag{8}$$

with $\forall k, l \in \mathbb{N} \,|\, k > l$,

$$t_k - t_l = \frac{(k - l + 1)}{f_0} - \frac{\phi(t_k) - \phi(t_l)}{2 \cdot \pi \cdot f_0}$$

Then, by applying the Wiener-Khintchine theorem as it is explained in the Appendix 1, we can say that[1]:

$$\sigma_N^2 = \frac{8}{\pi^2 \cdot f_0^2} \cdot \int_0^{+\infty} S_\phi(f) \cdot \sin^4(\frac{\pi \cdot f \cdot N}{f_0}) \cdot df \tag{9}$$

where $S_\phi(f)$ is the PSD of ϕ, which is the only unknown quantity in this equation.

By a study of a standard CMOS inverter let us now try to determine its theoretical value.

1) Theoretical value of $S_\phi(f)$:

During the past 20 years, numerous works such as [15], [16] and [17] tried to understand how noise currents present in all transistors of an oscillator are transformed into the jitter. Hadjimiri's work [17] is often referenced in this field. He shows that the impact of i_{ds} on ϕ can be reasonably modeled by a linear time variant system whose impulse sensitivity function is periodic. This model allows us to establish that a sinusoidal noise current whose frequency is ν and whose amplitude is I_i will be translated in term of excess phase by a sinusoidal signal whose frequency is $f = \nu \mod f_0$ and whose amplitude is $\frac{I_i \cdot d_m}{2 \cdot C_L \cdot V_{DD} \cdot f}$, where $m = \lfloor \frac{\nu}{f_0} \rfloor$, C_L is the load capacitance and d_m is the Fourier coefficient of the impulse sensitivity function. This way, Hadjimiri shows that when (1) is achieved, it is reasonable to say that:

$$S_\phi(f) = \frac{b_{fl}}{f^3} + \frac{b_{th}}{f^2} \tag{10}$$

Where b_{fl} and b_{th} are positive constants which fit respectively with the impact of the flicker and thermal noise on the excess phase.

[1]By writing this equation, we implicitly assume the average power of s_N is bounded

2) Calculation of σ_N^2:

By using (10) in (9), we can write:

$$\sigma_N^2 = \frac{8}{\pi^2 \cdot f_0^2} \cdot \int_0^{+\infty} \left[\frac{b_{fl}}{f^3} + \frac{b_{th}}{f^2}\right] \cdot \sin^4(\frac{\pi \cdot f \cdot N}{f_0}) \cdot df$$

The calculation of this integral allows us to establish that:

$$\sigma_N^2 = \frac{2 \cdot b_{th}}{f_0^3} \cdot N + \frac{8 \cdot \ln(2) \cdot b_{fl}}{f_0^4} \cdot N^2 \tag{11}$$

In this expression we define:

- $\sigma_{Nth}^2 := \frac{2 \cdot b_{th}}{f_0^3} \cdot N$: the thermal noise impact
- $\sigma_{Nfl}^2 := \frac{8 \cdot \ln(2) \cdot b_{fl}}{f_0^4} \cdot N^2$: the flicker noise impact

D. From noise currents to the independence of jitter realizations

Regarding (11), the linearity of σ_N^2 is only due to the thermal noise. This shape is predominant when N is low. For larger values, the impact of the flicker noise becomes most important and it causes a proportionality of σ_N^2 with N^2. We noticed in Section III-B that if $\{J(t_k)\}_{k=i\cdots i+2N-1}$ are mutually independent, then σ_N^2 is proportional to N . But for larger values of N and due to the flicker noise, this property is not verified. By this way, we can claim that flicker noise makes jitter realizations mutually dependent for large values of N.

To verify this result predicted by the theory, we propose to plot the shape of σ_N^2 as a function of N with experimental data.

E. Experimental validation

We implemented a differential jitter measurement circuitry depicted in Fig. 6 on the Evariste II benchmark platform featuring Altera Cyclone III FPGA [18].

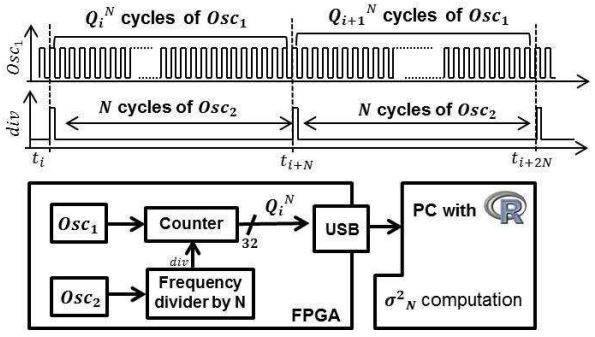

Fig. 6. Measurement circuit

It is composed of two identical rings oscillators (the same number of inverters in both ROs): Osc_1 and Osc_2 oscillating at a mean frequency of 103MHz. Let Q_i^N be the number of Osc_1 rising edges during N cycles of Osc_2 counted from time t_i as it is presented in Fig. 6. Thus, we are able to measure the relative jitter between Osc_1 and Osc_2 and we can establish that:

$$s_N(t_i) = \frac{Q_{i+1}^N - Q_i^N}{f_0} \tag{12}$$

Experimental results are depicted in Fig 7. The results confirm that in the case of our experiment, (11) can be considered as valid. Moreover the non-proportionality of σ_N^2 with large values of N highlights that, in this experiment, realizations of the jitter are not independent.

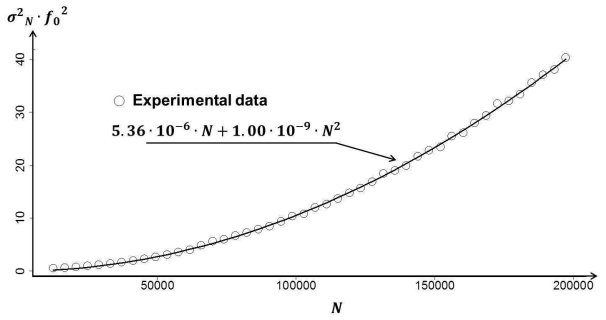

Fig. 7. Measurement circuit

Let $r_N = \frac{\sigma_{Nth}^2}{\sigma_N^2}$ be the ratio between the impact of the thermal noise and all the noises contained in s_N. In the case of our experiment, we can say that:

$$r_N = \frac{5354}{5354 + N}$$

We can use this ratio to set a threshold on N in order to reasonably assume that under this threshold, $2N$ consecutive jitter realizations are mutually independent. For instance, if $r_N > 95\%$ meaning that 95% of the total noise is due to the thermal noise contribution, we can say that they are almost mutually independent if $N < 281$.

With technological improvements on transistor shrinking, the flicker noise is expected to dominate further over the thermal noise making the r_N ratio decreasing for a given N. The flicker noise domination will further decrease the threshold, below which we can assume with sufficiently high precision that jitter realizations are mutually independent.

This results in a paradox. On one hand, the thermal noise contribution to the jitter will be less significant and will need much longer accumulation time to become measurable. On the other hand, increasing the number of periods will cause that the flicker noise will dominate even more and the measurement of the thermal noise contribution will be very hard to perform.

In the next section, we will show how our multi-level approach could help in measuring the thermal noise contribution to the jitter.

IV. Using the multi-level approach for measuring thermal noise contribution to the jitter

A. Principle

According to (11) and the fit obtained in Fig. 7 with experimental data:

$$\sigma_N^2 \cdot f_0^2 = \frac{2 \cdot b_{th}}{f_0} \cdot N + \frac{8 \cdot \ln(2) \cdot b_{fl}}{f_0^2} \cdot N^2$$

and knowing the frequency f_0, we can compute b_{th} and b_{fl}. If we are only interested in evaluation of the contribution of the thermal noise, we can say on one hand that

$$\sigma_N^2 = \sigma_{Nth}^2 = \frac{2 \cdot b_{th}}{f_0^3} \cdot N$$

and on the other hand we showed in Section III-B2 that if the period jitter is influenced only by the thermal noise, the jitter realizations are independent and so (6) holds

$$\sigma_N^2 = 2 \cdot N \cdot \sigma^2$$

Thus we have

$$\sigma^2 = \frac{b_{th}}{f_0^3}$$

making the measurement of the thermal noise contribution to the period jitter σ possible and given by:

$$\sigma = \sqrt{\frac{b_{th}}{f_0^3}}$$

B. Experimental result

In our experimental setup, we have $f_0 = 103$MHz and according to the fit in Fig. 7 we have $f_0^2 \sigma_{Nth}^2 = 5.36 \cdot 10^{-6} N$. Thus

$$b_{th} = \frac{5.36 \cdot 10^{-6}}{2} f_0 = 276.04\text{Hz}$$

and

$$\sigma = \sqrt{\frac{276.04}{(103 \cdot 10^6)^3}} \approx 15.89\text{ps}$$

This gives the ratio (period jitter over the mean period)

$$\frac{\sigma}{T_0} = \sigma f_0 = 1.6\,{}^0\!/_{00},$$

which is close to our measurements obtained by other more expensive methods in [19].

V. Conclusion

In this paper, we extended the classical approach of stochastic TRNG modeling by replacing the initial assumptions concerning the raw random analog signal by a model based on the study of transistor level physical phenomena, which serve as the entropy source. The new model shows that former P-TRNG stochastic models were based on assumptions that need important refinements. Unfortunately, these models were used for entropy estimation, which is directly related to the security of the generator, since low entropy bits can be easily predicted. The entropy per bit at the generator output and in consequence also the security was thus much lower than expected.

The main difference between former stochastic models and our new approach comes from the fact that the flicker noise is taken into account in the new extended model. It is interesting to notice that up to now, the presumed independence of successive jitter realizations was explained very simply: many intrinsic noise sources at transistor level contribute to the Gaussian noise that is superposed on the RRAS. This remains to be true. However we've demonstrated that because of the

presence of the flicker noise, resulting Gaussian noise makes realizations of the jitter mutually dependent. This dependence was neglected up to now. However, since the flicker noise that is responsible for this dependence is related to the technology (its PSD is the inverse of the square of the channel length), it can be expected that the autocorrelated noise will become more and more important in future, as transistor technologies will continue to shrink.

Besides refinement of existing stochastic models, one of the main results of the paper lies in the fact, that the enhanced model enables to measure very simply and precisely the thermal noise. Since this measurement can be easily embedded in a logic device, it can be used for implementing fast and precise generator-specific statistical test. Such test, required by AIS31, could detect very quickly attacks targeting the entropy source. We plan to implement such a dedicated test in the near future.

ACKNOWLEDGMENT

This work is partially supported by the TOISE European project. The authors also wish to thank Mr. Jean Nicolai and Mr. Michel Agoyan for helpful discussions

APPENDIX: ANALYTIC VALUE OF σ_N^2

$$s_N(t_i) = -\frac{\phi(t_{i+2N}) - 2\cdot\phi(t_{i+N}) + \phi(t_i)}{2\cdot\pi\cdot f_0} \tag{13}$$

Let us assume that s_N is an ergodic wide-sense stationary process, by this way, we can calculate σ_N^2 using the following expression:

$$\sigma_N^2 = < s_N^2(t) > \tag{14}$$

where

$$< x(t) > := \lim_{T\to\infty} \frac{1}{T}\cdot\int_{\frac{-T}{2}}^{\frac{T}{2}} x(t)\cdot dt$$

Assuming that ϕ is an ergodic wide-sense stationary process, by this way we can say that:

$$< \phi^2(t_{i+2N}) > = < \phi^2(t_{i+N}) > = < \phi^2(t_i) >$$

$$< \phi(t_i)\cdot\phi(t_{i+N}) > = R_\phi(t_{i+N} - t_i)$$

$$< \phi(t_{i+2N})\cdot\phi(t_{i+N}) > = R_\phi(t_{i+2N} - t_{i+N})$$

$$< \phi(t_{i+2N})\cdot\phi(t_i) > = R_\phi(t_{i+2N} - t_i)$$

where $R_\phi(\tau)$ is the autocorrelation function of ϕ with lag τ. Let us also assume that

$$R_\phi(t_{i+N} - t_i) = R_\phi(t_{i+2N} - t_{i+N}) = R_\phi\left(\frac{N}{f_0}\right)$$

and

$$R_\phi(t_{i+2N} - t_i) = R_\phi\left(\frac{2\cdot N}{f_0}\right)$$

This assumption is reasonable because the jitter is always small comparing to the accumulation of N periods.

Thus using (13) in (14):

$$\sigma_N^2 = \frac{6\cdot R_\phi(0) + 2\cdot R_\phi(\frac{2\cdot N}{f_0}) - 8\cdot R_\phi(\frac{N}{f_0})}{(2\cdot\pi\cdot f_0)^4} \tag{15}$$

And applying the Wiener-Khintchine theorem on ϕ, we can rewrite (15):

$$\sigma_N^2 = \frac{2}{(2\cdot\pi\cdot f_0)^2}\int_{-\infty}^{\infty} S_\phi(f)\cdot[3+e^{\frac{-4\cdot\pi\cdot j\cdot N\cdot f}{f_0}} - 4\cdot e^{\frac{-2\cdot\pi\cdot j\cdot N\cdot f}{f_0}}]\cdot df \tag{16}$$

And simplify this integral:

$$\sigma_N^2 = \frac{8}{\pi^2\cdot f_0^2}\int_0^{\infty} S_\phi(f)\cdot\sin^4(\frac{\pi\cdot f\cdot N}{f_0})\cdot df \tag{17}$$

REFERENCES

[1] Allan, D. W. (1966). Statistics of Atomic Frequency Standards. Proceedings of IEEE. pages 221230. , Vol. 54, No 2, February 1966.

[2] Allan, D. W. (1987). Should the classical variance be used as a basic measure in standards metrology?. Instrumentation and Measurement, IEEE Transactions on, 1001(2), 646-654.

[3] Markettos, A. T., Moore, S. W. (2009). The frequency injection attack on ring-oscillator-based true random number generators. In Cryptographic Hardware and Embedded Systems-CHES 2009 (pp. 317-331). Springer Berlin Heidelberg.

[4] Bayon, P., Bossuet, L., Aubert, A., Fischer, V., Poucheret, F., Robisson, B., Maurine, P. (2012). Contactless electromagnetic active attack on ring oscillator based true random number generator. In Constructive Side-Channel Analysis and Secure Design (pp. 151-166). Springer Berlin Heidelberg.

[5] Bernard, F., Fischer, V., Valtchanov, B. (2010). Mathematical model of physical RNGs based on coherent sampling.

[6] Amaki, T., Hashimoto, M., Mitsuyama, Y., Onoye, T. (2011). A design procedure for oscillator-based hardware random number generator with stochastic behavior modeling. In Information Security Applications (pp. 107-121). Springer Berlin Heidelberg.

[7] Sunar, B., Martin, W. J., Stinson, D. R. (2007). A provably secure true random number generator with built-in tolerance to active attacks. Computers, IEEE Transactions on, 56(1), 109-119.

[8] Baudet, M., Lubicz, D., Micolod, J., Tassiaux, A. (2011). On the security of oscillator-based random number generators. Journal of cryptology, 24(2), 398-425.

[9] Ben-Romdhane, M., Graba, T., Danger, J. L. (2013). Stochastic Model of a Metastability-Based True Random Number Generator. In Trust and Trustworthy Computing (pp. 92-105). Springer Berlin Heidelberg.

[10] W. Schindler and W. Killmann. (2011) A proposal for: Functionality classes for random number generators, September 2011

[11] K. Lundberg Noise sources in bulk CMOS (2002).

[12] R.Brederlow and G. Wenig and R. Thewes. Investigation of the thermal noise of MOS transistors under analog and RF operating conditions. In: Proc. 32th Eur. Solid-State Device Reseach Conf. (ESSDERC). 2002

[13] K. Hung and P. Ko. And C. Hu. Flicker noise characteristics of advanced MOS technologies. In: Electon Device Meeting, 1998. IEDM88. Technical Digest, International. IEEE, 1998 p.34-37.

[14] Boris Drakhlis, "Calculate Oscillator Jitter by using Phase-Noise Analysis Part 2," Microwaves and RF, February 2001, p. 109,

[15] McNeill, J. A. (1997). Jitter in ring oscillators. Solid-State Circuits, IEEE Journal of, 32(6), 870-879.

[16] Abidi, A. A. (2006). Phase noise and jitter in CMOS ring oscillators. Solid-State Circuits, IEEE Journal of, 41(8), 1803-1816.

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

[18] Fischer, V., Haddad, P., Bernard, F. (2013). An open-source multi-FPGA modular system for fair benchmarking of true random number generators. In Proceedings of the 23rd international conference on field programmable logic and applications.

[19] Lubicz, D., Bochard, N. Towards an oscillator based TRNG with a certified entropy rate.