A Physical Approach for Stochastic Modeling of TERO-based TRNG

Patrick Haddad, Viktor Fischer, Florent Bernard, Jean Nicolai

A Physical Approach for Stochastic Modeling of TERO-based TRNG

Patrick Haddad[1,2], Viktor Fischer[1], Florent Bernard[1] and Jean Nicolai[2]

[1] Laboratoire Hubert Curien,
Université Jean Monnet, Member of Université de Lyon,
F-42000 Saint-Etienne, France
Email: (patrick.haddad, fischer, florent.bernard)@univ-st-etienne.fr

[2] STMicroelectronics
Advanced System Technology
F-13790 Rousset , France
Email: jean.nicolai@st.com

Abstract. Security in random number generation for cryptography is closely related to the entropy rate at the generator output. This rate has to be evaluated using an appropriate stochastic model. The stochastic model proposed in this paper is dedicated to the transition effect ring oscillator (TERO) based true random number generator (TRNG) proposed by Varchola and Drutarovsky in 2010. The advantage and originality of this model is that it is derived from a physical model based on a detailed study and on the precise electrical description of the noisy physical phenomena that contribute to the generation of random numbers. We compare the proposed electrical description with data generated in a 28 nm CMOS ASIC implementation. Our experimental results are in very good agreement with those obtained with both the physical model of TERO's noisy behavior and with the stochastic model of the TERO TRNG, which we also confirmed using the AIS 31 test suites. [1]

Keywords: hardware random number generators, transition effect ring oscillator, stochastic models, entropy, statistical tests

1 Introduction

Random number generation is a critical issue in most cryptographic applications. Random numbers are used as confidential keys, but also as initialization vectors, challenges, nonces, and random masks in side channel attack countermeasures. A security flaw in random number generation has a direct impact on the security of the whole cryptographic system. Contrary to generators used in Monte Carlo simulations and telecommunications, those designed for cryptography must generate unpredictable random numbers – having perfect statistical properties is necessary but not sufficient.

There are two main categories of random number generators: deterministic random number generators (DRNG) and true random number generators (TRNG), which can be physical (P-TRNG) or non-physical (NP-TRNG). While deterministic generators are based on algorithmic processes and are thus not truly random, TRNGs exploit an unpredictable process, such as analog phenomena in electronic devices, to produce a random binary sequence or a sequence of random numbers. The unpredictability of DRNGs is guaranteed computationally and that of TRNGs is guaranteed physically. A good knowledge of the underlying physical process in TRNG that ensures its randomness and hence its unpredictability is therefore necessary.

The statistical quality of TRNGs and DRNGs is usually evaluated using statistical test suites such as the one first proposed by George Marsaglia [6] and extended by the NIST [8]. The goal of these suites is to detect statistical weaknesses such as non-uniformity or the appearance of patterns in a generated random sequence of only limited size. In no case can these tests guarantee the unpredictability of the random binary sequence.

As summarized by Fischer in 2012 [3], the best way to ensure unpredictability is to carefully estimate the entropy rate at the generator output. The estimation of entropy must be based on a carefully constructed model of the random number generation process. In a P-TRNG, this model consists of a mathematical description of a link between the variations in the exploited unpredictable analog phenomena and the variations in the random binary sequence.

The entropy estimation based on an underlying stochastic model is mandatory in the security certification process, specifically at high levels of security [5]. Stochastic models are reasonably easy to construct, but it is sometimes difficult or even impossible to check all the underlying physical assumptions. A physical model could serve as a basis for validation of these assumptions, but it is much more difficult to construct and a detailed knowledge of contributing physical phenomena is necessary.

Some stochastic models are generic and can be adapted to several generators [4], but many TRNGs require their own specific stochastic models. Unfortunately, only a few existing generators have corresponding stochastic models, e.g. [1], [10], [2]. One of the interesting generators recently proposed by Varchola and Drutarovsky [11] uses a so-called transient effect ring oscillator (TERO) as a source of randomness. Although the generator produces good statistical results, a corresponding stochastic model has not yet been proposed and the generic model proposed in [4] is clearly not suitable in this case.

Our contributions: 1) We propose and validate a novel physical TERO model including electric noises that serve as sources of randomness. 2) From the physical model, we derive a TERO stochastic model. 3) From the TERO model, we propose and validate a stochastic model of a complete TERO-based TRNG and illustrate the use of this model to estimate the entropy rate in conjunction with the output bit rate.

Organization of the paper: In Section 2, we describe the structure of the TERO and its use in a P-TRNG. The physical (electrical) and derived stochastic model of the TERO are detailed in Section 3. The stochastic model of the complete TERO-based TRNG is presented in Section 4. We conclude the paper by a discussion concerning the relationship between the entropy rate and the output bit rate that can be set up using the proposed stochastic model.

2 The TERO based RNG – background

The TERO is an electronic circuit that oscillates temporarily. It is composed of an even number of inverters and a couple of gates that restart temporary oscillations (e.g. two NAND or two XOR gates). A typical TERO configuration is presented in the left panel of Fig. 1: it is composed of two NAND gates and two inverter branches. The TERO can be seen as an RS latch with two inputs featuring the same voltage V_{ctr} and two different outputs V_{out1} and V_{out2}.

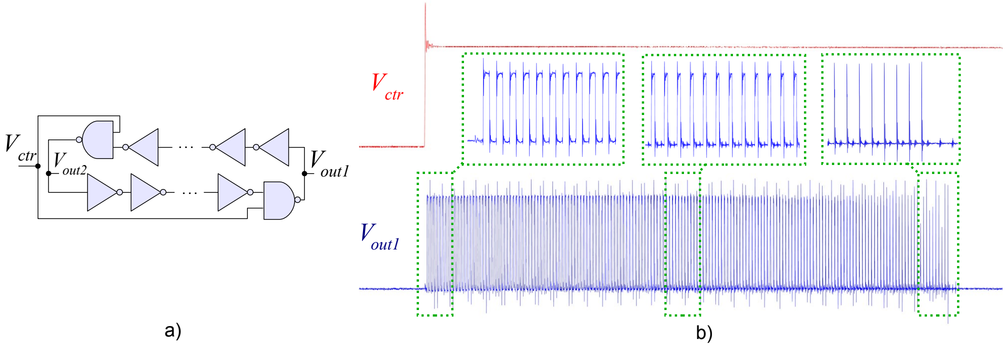

Fig. 1. Circuit diagram of a typical TERO structure and its input/output waveforms obtained experimentally

Following the rising edge of the V_{ctr} input, the outputs V_{out1} and V_{out2} start to oscillate. The oscillations have a constant mean frequency, but their duty cycle varies over time: it changes monotonously and after a certain number of oscillations, it reaches the rate of either 0% or 100%. At this point, outputs V_{out1} and V_{out2} stop oscillating and remain stable at two opposite logic values. The right panel of Fig. 1 presents traces of the V_{ctr} input and V_{out1} output signal captured from oscilloscope.As can be observed, the output signal V_{out1} starts to oscillate following the rising edge of the V_{ctr} control signal.

The three zooms presented in this panel show the changing duty cycle: immediately after the rising edge of the V_{ctr} signal, it is close to 50%, then decreases until it reaches 0%. Consequently, signal V_{out1} stabilizes at logic level 0. Of course, signal V_{out2} behaves in the opposite way as far as the duty cycle is concerned and stabilizes at logic level 1.

The number of oscillations before the outputs stabilize is not constant but varies because it is impacted by the electronic noises that disturb the normal behavior of transistors in the TERO structure.

The P-TRNG based on the TERO structure (TERO TRNG) is depicted in Fig. 2. The TERO circuitry is followed by an n-bit counter that counts the rising edges of the temporary oscillations. The counter output shows realizations of the random variable, i.e. the number of oscillations in successive control periods. The random binary sequence is usually obtained by successively concatenating the least significant bits of the counter, i.e. only one T flip-flop is needed in the counter.

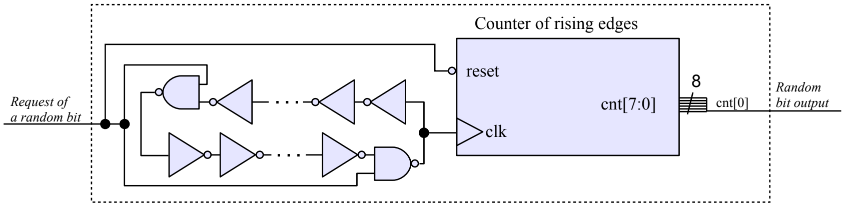

Fig. 2. True random number generator based on the TERO structure

To evaluate the physical parameters of the TERO TRNG, we implemented the generator in a CMOS BULK ASIC using the ST Microelectronics 28 nm technology. In our configurations, one of the two outputs of the TERO structure was connected to an 8-bit asynchronous counter. Figure 3 shows the distribution of the 8 million counter values obtained from the ASIC device for two different TERO topologies: in the first one, there was a relative difference between the two TERO branches of 24 % (left panel) and in the second one a relative difference 31 % (right panel). The differences between the TERO branches were obtained using a digital configurable delay chain.

It can be seen that in both cases the number of oscillations varied around a mean value according to a statistical law, which apparently is not a normal law. This is especially visible in the right panel of the figure. One of our objectives was to determine this law and its origin.

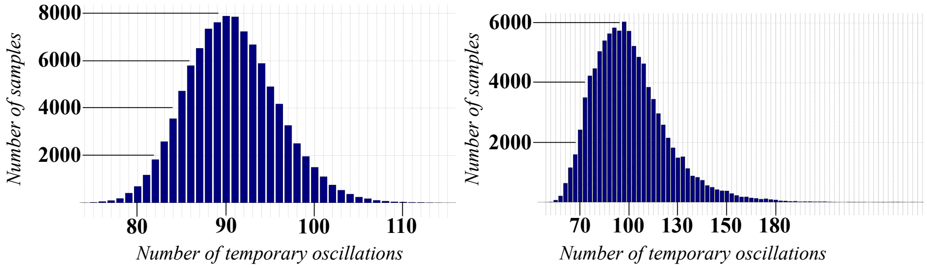

Fig. 3. Distribution of numbers of temporary oscillations for two TERO topologies in technology ST 28 nm: with the relative difference in delay between the two TERO branches of 24 % (left panel) and with the relative difference 31 % (right panel)

Before proceeding with the construction of the physical and stochastic models, we tested the statistical quality of generated bit streams. The bit streams obtained by successive concatenation of the least significant bits constituted the raw binary streams, which were then tested using the AIS31 protocol [KS11]. The data not only successfully passed all the tests of the Procedure B, but also those of the Procedure A aimed at testing the post-processed signals. This means that the generator is suitable for certification according to AIS31 for PTG1 and PTG2 levels even without post-processing.

As explained above, successful evaluation of the output of the generator using statistical tests is a necessary but not sufficient condition to ensure the unpredictability of the generated numbers. The only way to guarantee such a property is to show the link between variations in the distribution of the raw random binary sequence and the physical phenomena that are considered as random, unpredictable, and non-manipulable. Statistical modeling of underlying analog and digital processes should make it possible to quantify the uncertainty included in the generated random sequence by estimating the entropy rate in this sequence.

3 Physical and stochastic model of TERO

In this section, we discuss the main processes that transform noisy electric currents into random binary sequences and explain how these phenomena are interlinked.

3.1 Modeling the number of temporary oscillations

Our study is based on an existing physical model of RS latches published by Reyneri *et al.* in [7]. We complete their noise free model by taking electric noises into account. For the sake of readability, the original model of the noise free inverter is presented in Appendix A.

Modeling a noisy inverter Noisy behavior at transistor level is modeled by noisy currents that are added to the ideal noise-free current flowing between the source and the drain. As can be seen in Fig. 4 a) for a CMOS inverter, these noisy currents can be represented by two sources of current n_N and n_P, which are connected in parallel to output transistors and which are active only during inverter (gate) switching.

The inverter's noisy output V_{out} can be seen as a sum of two signals – $f(t)$ and $n(t)$:

- $f(t)$ represents an ideal component of the output signal, which contributes to the charge and discharge of the C_L capacitor by noise-free switching currents between the source and drain of output transistors MN and MP
- $n(t)$ corresponds to the noisy component of the output signal, i.e. it contributes to the charge and discharge of the C_L by the noisy signals n_N and n_P.

Let t_0 be the last moment at which V_{out} is equal to V_{CC}. Since the noisy currents exist only during gate switching, $n(t_0) = 0$. It is therefore clear that:

$$n(t) = n(t) - n(t_0) = \frac{1}{C_L}\int_{t_0}^{t}[n_N(u) + n_P(u)]du$$

In the following, we assume that n_N and n_P are Gaussian random variables. This assumption is reasonable, because the noise currents can be considered as sums of ran-

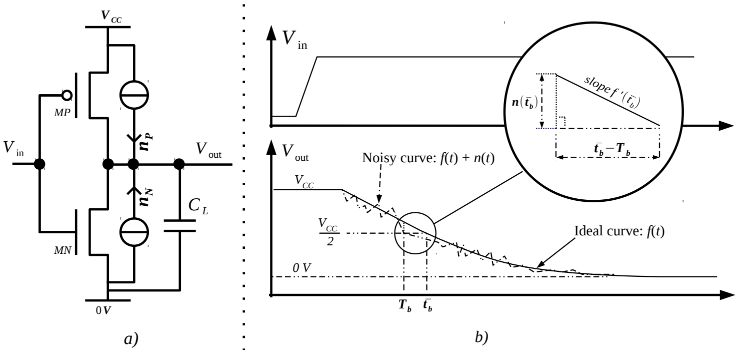

Fig. 4. Model of a noisy inverter and its response to a step function

dom variables associated with independent quantum processes in the transistors. Consequently, $n(t)$ can be represented as a stationary Gaussian random process[2].

Let us now analyze modifications in length of the pulse transmitted over one inverter as explained in Appendix A, but now in the presence of noisy currents. Let us consider that at $t = t_{\downarrow}$, signal V_{in} goes down from V_{CC} to 0 ,and we denote t_a the time, at which the signal V_{out} at the output of the inverter reaches $\frac{V_{CC}}{2}$. Similarly, at $t = t_{\uparrow}$, signal V_{in} goes up from 0 to V_{CC} and t_b corresponds to the time at which V_{out} is equal to $\frac{V_{CC}}{2}$. Finally, at $t = t_{end}$ signal V_{in} goes back to 0, ending one cycle. We denote $t_c = t_{end} - t_{\downarrow}$ the time that V_{in} needs to complete one cycle. For the sake of simplicity, we will denote p_{in} the length of one pulse at signal V_{in} and p_{out} the corresponding pulse at the output of an open chain of inverters.

Proofs of the following lemma and propositions are given in Appendix B.

Lemma 1 *Let T_a (resp. T_b) be the random variable representing the time at which the signal V_{out} reaches $\frac{V_{CC}}{2}$ after a falling edge (resp. rising edge) on V_{in}. Let $\overline{t_a}$ (resp. $\overline{t_b}$) denote the ideal time at which V_{out} should reach $\frac{V_{CC}}{2}$ in noise-free conditions. Let P_{out} be the random variable representing the length of a pulse at signal V_{out} corresponding to a pulse of length p_{in} at signal V_{in}. Then, with previous definitions of signals $f(t)$ and $n(t)$, we have:*

1. $T_a \sim \mathcal{N}\left(\overline{t_a},\, \frac{\sigma^2}{f'\left(\overline{t_a}\right)}\right)$ *and* $T_b \sim \mathcal{N}\left(\overline{t_b},\, \frac{\sigma^2}{f'\left(\overline{t_b}\right)}\right)$
2. *If T_a and T_b are independent,*

$$P_{out} \sim \mathcal{N}(\mu_{out},\, \sigma^2_{out}) \text{ with } \begin{cases} \mu_{out} = \frac{t_c}{2} + \left(p_{in} - \frac{t_c}{2}\right)(1 + H_d) \\ \sigma^2_{out} = \sigma^2 \left(\frac{1}{f'\left(\overline{t_a}\right)} + \frac{1}{f'\left(\overline{t_b}\right)}\right) \end{cases}$$

where H_d is the constant introduced in Appendix A.

[2] This may be not true at the device startup, but this assumption is reasonable after some time t_0. For each $t \geq t_0$, we assume that $n(t)$ follows a normal distribution with mean 0 and variance σ^2, denoted $n(t) \sim \mathcal{N}(0, \sigma^2)$ in the following.

Shortening of the pulse while it traverses a delay chain Let us now consider an open chain of N inverters discussed in the previous section, where N is a non-zero positive integer. Let V_{in} be the input signal of the first inverter and V_{out_N} the output signal of the N^{th} inverter. P_{out_N} is the length of a pulse at V_{out_N} corresponding to a pulse p_{in} at signal V_{in}. The random behavior of P_{out_N} is given in Proposition 1.

Proposition 1 *If the noise source in the inverter is independent from the noise sources in other inverters, then*

$$P_{out_N} \sim \mathcal{N}(\mu_{out_N}, \sigma^2_{out_N}) \text{ with } \begin{cases} \mu_{out_N} = \frac{t_c}{2} + \left(p_{in} - \frac{t_c}{2}\right)(1+H_d)^N \\ \sigma^2_{out_N} = \sigma^2_{out}\left(\frac{(1+H_d)^{2N}-1}{(1+H_d)^2-1}\right) \end{cases}$$

Modeling temporary oscillations in the TERO structure Let us now consider two chains of inverters, as discussed in the previous section. Let $\{K_j\}_{j=1\ldots 2M}$ represent the set of inverters in the first chain and $\{L_j\}_{j=1\ldots 2M}$ those in the second chain. We denote NK and NL the two NAND gates with outputs V_K and V_L. They are connected to chains $\{K_j\}_j$ and $\{L_j\}_j$ (as depicted in Fig. 5 a)) and complete a TERO. If V_{ctr} is equal to V_{CC}, NL (resp. NK) can be seen as the L^{th}_{2M+1} (resp. K^{th}_{2M+1}) inverter of the chain $L := \{L_j\}_{j=1\ldots 2M+1}$ (resp. $K := \{K_j\}_{j=1\ldots 2M+1}$) generating the mean delay τ_1 (resp. τ_2). Theoretically, τ_1 and τ_2 are identical, since both branches have the same topology. In practice, because of imperfections in the manufacturing process, their values differ slightly. Without any loss of generality, we can assume that $\tau_1 > \tau_2$.

At $t = 0$, let signal V_{ctr} go up from 0 to V_{CC}. As shown in Fig 5 b), this rising edge forces the outputs of NAND gates NK and NL to fall from V_{CC} to 0. The falling edge created at V_K (resp. at V_L) propagates over K (resp. L). This creates a pulse of mean length τ_1 (resp. τ_2) at V_L (resp. V_K).

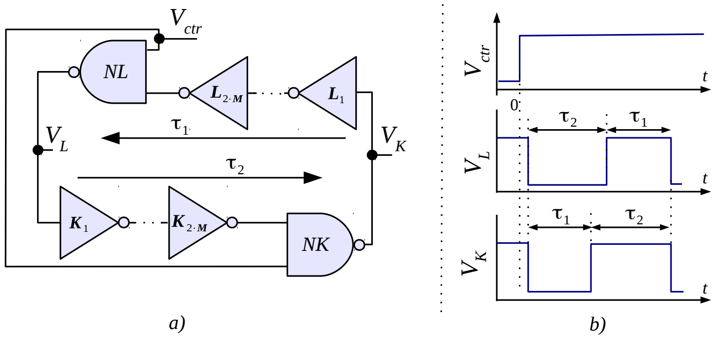

Fig. 5. Initial behavior of the TERO structure

The two rising edges created on V_L and V_K start to propagate over elements L and K. After a mean delay τ_2 (resp. τ_1), they cause signal V_L (resp. V_K) to fall from V_{CC} to 0. The generated signals behave in the same way as the signals traversing set $\{I_j\}$ in the previous section with a cycle of length $t_c = \tau_1 + \tau_2$.

Proposition 2 *Let PL_0 (resp. PK_0) be the length of the pulse observed at signal V_L (resp. V_K) and PL_S (resp. PK_S) be the pulse length, once it has crossed S times over both sets K and L.*
If $PL_0 \sim \mathcal{N}(\tau_2,\, \sigma^2_{out_{2M+1}})$ and $PK_0 \sim \mathcal{N}(\tau_1,\, \sigma^2_{out_{2M+1}})$ and if the noise sources in all the inverters are independent, then

$$PL_S \sim \mathcal{N}(\mu_{L_S},\, \sigma^2_{L_S}) \text{ with } \begin{cases} \mu_{L_S} &= \frac{\tau_1+\tau_2}{2} + \frac{\tau_2-\tau_1}{2} R^S \\ \sigma^2_{L_S} &= \sigma^2_{out} \dfrac{R^{2S+1}-1}{(1+H_d)^2-1} \end{cases}$$
$$PK_S \sim \mathcal{N}(\mu_{K_S},\, \sigma^2_{K_S}) \text{ with } \begin{cases} \mu_{K_S} &= \frac{\tau_1+\tau_2}{2} + \frac{\tau_1-\tau_2}{2} R^S \\ \sigma^2_{K_S} &= \sigma^2_{out} \dfrac{R^{2S+1}-1}{(1+H_d)^2-1} \end{cases}$$

where $R = (1+H_d)^{4M+2}$.

According to Proposition 2, $\mu_{L_S} + \mu_{K_S} = \tau_1 + \tau_2$. So the mean values of the duty cycles of signals V_K and V_L are always complementary. Since by definition, PL_S represents the length of the pulses observed at signal V_L and because of our assumption that $\tau_1 > \tau_2$, oscillations disappear when $PL_S = 0$. Consequently, the number of oscillations N_{OSC} corresponds to the last value of S for which PL_S is positive:

$$N_{OSC} = \max\{S | PL_S > 0\}. \tag{1}$$

Let q be a positive integer different from zero. From Eq. (1) it follows that if N_{OSC} is greater than q, then PL_q is positive and different from zero, too. Using this fact, we can derive the probability that N_{OSC} is greater than q from Proposition 2:

$$Pr\{N_{OSC} > q\} = Pr\{PL_q > 0\}. \tag{2}$$

Then

$$Pr\{N_{OSC} > q\} = \frac{1}{\sqrt{2\pi}\sigma_{L_S}} \int_{[\frac{\tau_1-\tau_2}{2}]R^q - \frac{\tau_1+\tau_2}{2}}^{+\infty} \mathrm{e}^{-\frac{u^2}{2\sigma^2_{L_S}}} \mathrm{d}u, \tag{3}$$

or equivalently

$$Pr\{N_{OSC} > q\} = \frac{1}{2}\left[1 - erf\left(\frac{[\tau_1-\tau_2]R^q - \tau_1 - \tau_2}{2\sqrt{2}\sigma_{out}\sqrt{\frac{R^{2q+1}-1}{(1+H_d)^2-1}}}\right)\right]. \tag{4}$$

Finally, from Eq. (4) we get the probability that N_{OSC} is smaller or equal to q:

$$Pr\{N_{OSC} \le q\} = 1 - Pr\{N_{OSC} > q\} = \frac{1}{2}\left[1 - erf\left(K\frac{1-R^{q-q_0}}{\sqrt{R^{2q+1}-1}}\right)\right], \tag{5}$$

where K and q_0 are equal to:

$$K = \frac{\sqrt{R^2-1}}{2\sqrt{2}\sigma_r}, \tag{6}$$

$$q_0 = -\frac{\log(\mathit{\Delta}_r)}{\log(R)}, \tag{7}$$

and where

$$\sigma_r = \sigma_{out}\sqrt{\frac{R^2-1}{(1+H_d)^2-1}}/(\tau_1+\tau_2) = \sigma_{out_{4M+2}}/(\tau_1+\tau_2),$$

$$\mathit{\Delta}_r = (\tau_1-\tau_2)/(\tau_1+\tau_2).$$

Using Eq. (5), the probability p_q that N_{OSC} is equal to q can be estimated by

$$p_q = Pr\{N_{OSC} \leq q\} - Pr\{N_{OSC} \leq q-1\},$$

$$p_q = \frac{1}{2}\left[erf\left(K\frac{1-R^{q-q_0-1}}{\sqrt{R^{2q}-1}}\right) - erf\left(K\frac{1-R^{q-q_0}}{\sqrt{R^{2q+2}-1}}\right)\right]. \tag{8}$$

Equation (8) is very important, because it can be used to model the distribution of the number of temporary oscillations. Its main advantage is that the parameters of the model (R, σ_r and $\mathit{\Delta}_r$) are easy to quantify (see Section 3.2). Parameter R is the ratio of the geometric series, σ_r is the relative jitter and $\mathit{\Delta}_r$ is the relative difference between TERO branches. The proposed model, as we will see later, can serve as a basis for the TERO TRNG stochastic model.

3.2 Experimental validation of the TERO stochastic model

We validated the TERO model using the two TERO topologies presented in Sec. 2. We evaluated the appropriateness of the model using 65536 realizations $\{A_k\}_{k=1\ldots65536}$ of the TERO temporary oscillations. The model parameters R, $\mathit{\Delta}_r$, and σ_r were computed from acquired data by determining K and q_0 from Eq. (6) and (7) as follows.

First, an approximation of the distribution of temporary oscillations N_{OSC} is obtained experimentally, the distribution $Pr\{N_{OSC} \leq q\}$ can be thus computed. Then, according to Eq. (5), the function

$$Y(q) = erf^{-1}\Big(1-2Pr\{N_{OSC} \leq q\}\Big) = K\frac{1-R^{q-q_0}}{\sqrt{R^{2q+2}-1}} \tag{9}$$

is obtained from the distribution $Pr\{N_{OSC} \leq q\}$. It is then possible to find the value of q_0 such that $Pr\{N_{OSC} \leq q\} = 1/2$. Finally, the value of R is determined. Knowing that $R \sim 1$ and $R > 1$, we are searching in a loop for $R > 1$ in a neighborhood of 1 the value R_{loop}, such that the ratio $Y(q)/Z(q)$ is constant (i.e. independent from q). This constant represents the value of K. As mentioned above, Y(q) is obtained experimentally and Z(q) is derived from Eq. (9) as follows:

$$Z(q) = \frac{1-R_{loop}^{q-q_0}}{\sqrt{R_{loop}^{2q+2}-1}} \tag{10}$$

The results are presented in Fig. 6. The distribution depicted in the left panel was obtained using parameter values: $R = 1.0153$; $\mathit{\Delta}_r = 0.2394$; $\sigma_r = 0.00174$ and the distribution shown in the right panel was modeled with parameters: $R = 1.013$; $\varDelta_r = 0.310$; $\sigma_r = 0.0059$.

Next, we compared the model from Eq. (5) with the distribution of the experimental data $\{A_k\}$ obtained with the two hardware configurations using the χ^2 goodness-of-fit test. For the distribution presented in the left panel of Fig. 6, the counter values varied between 74 and 110, which corresponded to 38 degrees of freedom and the χ^2 test statistic was $T = 40.35$. At 38 degrees of freedom and a significance level $\alpha = 0.05$, for a good fit, the χ^2 test statistic T should be below 53.384, i.e. $Pr\{T < 53.384\} = 0.95$. Similarly, for the distribution presented in the right panel featuring 76 degrees of freedom, the χ^2 test statistic was equal to $T = 33.97$. At 76 degrees of freedom, for the same significance level, the threshold of the χ^2 test statistic is 97.351, i.e. $Pr\{T < 97.351\} = 0.95$.

In these two cases, but also in all the other experiments the χ^2 test statistic value T was below the threshold corresponding to the level of significance $\alpha = 0.05$. We can thus conclude that the model presented in Sec. 3.1 is suitable for the characterization of the probability distribution of the number of TERO oscillations N_{OSC}.

Just out of curiosity, we compared the two distributions with the distribution of the normal law. The χ^2 test statistics were $T = 149.3$ and $T > 2 \cdot 10^6$, respectively. In both cases, and especially in the second, the test statistic was clearly outside the required interval.

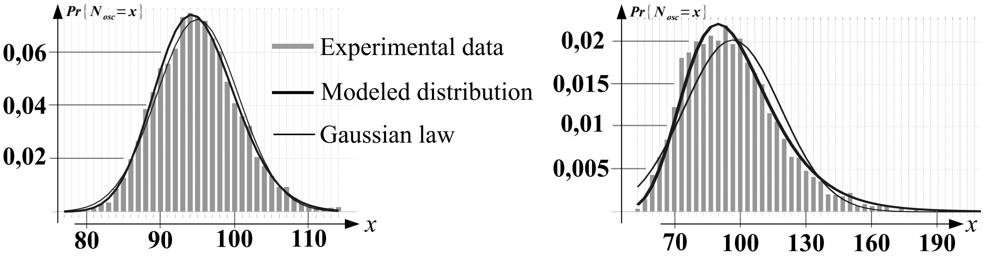

Fig. 6. Experimental validation of the model for two TERO topologies in technology ST 28 nm: with the relative difference in delay between the two TERO branches of 24 % (left panel) and with the relative difference 31 % (right panel)

In the next section, we will use our model to estimate entropy at the TERO TRNG output.

4 Stochastic model of the complete TERO-based TRNG

Let H_{osc} be the entropy contained in the sequence of number of oscillations N_{osc}. Since realizations of N_{osc} are assumed to be independent (the generator is restarted periodically and it is thus memory-less), this entropy is related to p_q from Eq. (8) as follows:

$$H_{N_{osc}} = -\sum_{q \in \mathbb{N}} p_q \log_2(p_q)$$

We computed the value of $H_{N_{osc}}$ for the two distributions depicted in Fig. 6. The distribution shown in the left panel had the entropy rate per sample (per byte) $H_{N_{osc}} = 4.47$ and that in the right panel had the entropy rate $H_{N_{osc}} = 6.32$.

Let p_b be the probability that the least significant bit of N_{osc} is equal to 1. This probability is related to p_q from Eq. (8) as follows:

$$p_b = \sum_{k=0}^{k=+\infty} p_{2k+1}. \tag{11}$$

For each realization, we select the least significant bit of N_{osc} to form a vector $(b_{n-1} \dots b_0)_2$. This vector can be interpreted as a number $B_n \in \{0, \dots, 2^n - 1\}$. As the TRNG is restarted after each acquisition of N_{osc}, bits $(b_k)_{k=0 \dots n-1}$ are independent. Thus, for each n-bit integer $X_n = (x_{n-1} \dots x_1 x_0)_2$

$$p_{X_n} = Pr(B_n = X_n) = \prod_{j=0}^{n-1} [1 - p_b]^{1-x_j} [p_b]^{x_j}.$$

If the random process associated with B_n is stationary, the entropy per bit at the generator output is equal to [9]:

$$H = \lim_{n \to +\infty} \frac{H_n}{n},$$

where

$$H_n = - \sum_{X_n \in \{0, \dots, 2^n - 1\}} p_{X_n} \log_2(p_{X_n}).$$

Since jitter realizations are assumed to be independent, realizations of N_{osc} and b_k are assumed to be independent, too. Consequently, we consider that the generator does not have a memory and the generated random bits don't contain any short- or long-term dependencies.

Because realizations of b_k are considered to be independent, the entropy per bit at the generator output derived from our model can be simplified as follows:

$$H = -p_b \log_2(p_b) - (1 - p_b) \log_2(1 - p_b).$$

We computed the entropy rate per bit for the two TERO topologies discussed in Sec. 3.2. In both cases, the entropy rate was higher than 0.9999, meaning that the entropy per bit exceeded the value required by AIS 31. This was in perfect agreement with our experiments – results of the tests AIS 31 presented in Sec. 2.

5 Discussion

As we have seen above, the distribution of counter values is very well characterized by the model parameters R, σ_r, and Δ_r and the entropy of the generated sequence depends on this distribution. Using the model, we can now observe the impact of the TERO design on the distribution of random numbers and hence on entropy.

First, entropy is determined by relative jitter, i.e. by parameter σ_r. Since designers cannot directly alter the sources of thermal noise, they can only change the relative jitter by reducing the delay of the two TERO branches. This corresponds to increasing the frequency of oscillations.

Another important model parameter that determines entropy rate is the relative difference between the two TERO branches, i.e. parameter Δ_r. With smaller relative differences, TERO accumulates more jitter because it oscillates longer. As we have seen in our example, the entropy rate per generated output byte was over 4.4 and 6.3, respectively. This means that if designers use only one bit per generated byte (the counter output), they would be discarding a high percentage of usable random data. Of course, some post-processing can be used to profit from as much entropy as possible, but it would require additional silicon area, especially if a sophisticated algorithm is used (which would be probably the case in order to maintain a maximum entropy rate). Another much more practical solution would be to unbalance the two TERO branches to the extent that the entropy rate per generated byte would be slightly higher than 1 and then to use only one bit per generated number. Because of the difference in delays in the two branches, the TERO would oscillate a shorter time and the output bit rate would consequently be higher. Since the entropy rate per generated number would be higher than one, each generated bit (the least significant bit of the counter) would have enough entropy and post-processing would not be necessary.

6 Conclusion

In this paper, we analyzed the processes that transform the noisy currents in the TERO circuitry into a random bit stream of the TERO based TRNG. First, we performed a detailed analysis of electric processes inside the TERO structure and, based on this analysis, we proposed the physical model of the TERO. We checked the model in two specific TERO topologies implemented in an ST 28 nm ASIC technology.

Next, based on this model, we proposed a stochastic model of a complete TERO based TRNG. We showed that the proposed stochastic model can be successfully used to estimate the entropy rate. The entropy estimations are in perfect agreement with the results of the AIS 31 test suites.

We also showed that the proposed TRNG stochastic model can be used not only to estimate the entropy rate at the output of the generator, but also for entropy management, by setting sufficient entropy rate while maintaining the maximum output bit rate.

Acknowledgments

This work has received fundings from the European ENIAC Joint Undertaking (JU) in the framework of the project TOISE (Trusted Computing for European Embedded Systems) and from the European Union's Horizon 2020 research and innovation programme in the framework of the project HECTOR (Hardware Enabled Crypto and Randomness) under grant agreement No 644052.

The authors wish to thank Mr. Nicolas Bruneau, Mr. Michel Agoyan and Mr. Yannick Teglia for their help and availability in numerous discussions.

References

1. M. Baudet, D. Lubicz, J. Micolod, and A. Tassiaux. On the security of oscillator-based random number generators. *Journal of Cryptology*, 24(2):398–425, 2011.
2. F. Bernard, V. Fischer, and B. Valtchanov. Mathematical model of physical RNGs based on coherent sampling. *Tatra Mountains Mathematical Publications*, 45(1):1–14, 2010.
3. V. Fischer. A closer look at security in random number generators design. In *Constructive Side-Channel Analysis and Secure Design – COSADE 2012*, pages 167–182. Springer, 2012.
4. W. Killmann and W. Schindler. A Design for a Physical RNG with Robust Entropy Estimators. In Elisabeth Oswald and Pankaj Rohatgi, editors, *Cryptographic Hardware and Embedded Systems – CHES 2008*, volume 5154 of *LNCS*, pages 146–163. Springer, 2008.
5. W. Killmann and W. Schindler. A proposal for: Functionality classes for random number generators. Online. Available at: https://www.bsi.bund.de, 2011.
6. G. Marsaglia. DIEHARD: Battery of Tests of Randomness. Online. Available at: http://stat.fsu.edu/pub/diehard/, 1996.
7. L. M. Reyneri, D. Del Corso, and B. Sacco. Oscillatory metastability in homogeneous and inhomogeneous flip-flops. *Solid-State Circuits, IEEE Journal of*, 25(1):254–264, 1990.
8. A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications – NIST SP 800-22, rev. 1a, 2010.
9. C. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27:379–423, 623–656, July, October 1948.
10. B. Sunar, W. J. Martin, and D. R. Stinson. A Provably Secure True Random Number Generator with Built-In Tolerance to Active Attacks. *IEEE Transactions on Computers*, pages 109–119, 2007.
11. M. Varchola and M. Drutarovsky. New high entropy element for fpga based true random number generators. In *Cryptographic Hardware and Embedded Systems (CHES), 2010*, pages 351–365. Springer, 2010.

Appendix

A Modeling an ideal noise-free inverter

We assume that TERO is built using ideal noise-free CMOS inverters as presented in Fig. 7 a). We note V_{in} and V_{out} the input and output signal of such an inverter, respectively. The noise-free model is based on the physical model of an inverter with a variable slope published by Reyneri *et al.* in [7]. As presented in Fig. 7 b), the model proposed in [7] divides the inverter into three entities:

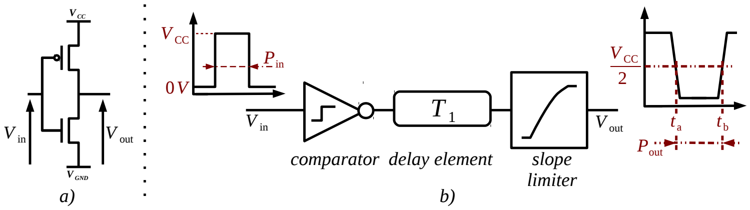

Fig. 7. Ideal noise-free CMOS inverter

- A comparator, which outputs V_{CC} if the input voltage V_{in} is smaller than $V_{CC}/2$ otherwise it outputs 0.
- A delay line, which delays comparator output signal by a static delay T_1.
- A slope limiter, which follows the delay line and generates the output signal V_{out}.

As depicted in Fig. 8, the model responds to a rising edge of the input signal by generating a signal that decreases linearly with the slope $-K_0$ until the output voltage reaches the value $(1 - K_0) \cdot V_{CC}$ [3] after which the output decreases exponentially until it reaches the final value V_{out}.

First, let we consider that at $t = 0$, signal V_{in} goes down from V_{CC} to 0 and $\overline{t_a}$ is the time at which the output signal V_{out} is equal to $\frac{V_{CC}}{2}$. At time $t = p_{in}$, signal V_{in} goes up from 0 to V_{CC} and at $\overline{t_b}$ output V_{out} is equal to $\frac{V_{CC}}{2}$. Finally, at $t = t_c$, V_{in} goes back to V_{GND}. Consequently, the length of the positive pulse at output V_{out} is equal to $p_{out} = \overline{t_b} - \overline{t_a}$.

The authors of [7] also describe the behavior of the inverter when the input signal has the same form as the described output signal. They show that in this case P_{out} can be approximated by:

$$p_{out} = \frac{t_c}{2} + \left[p_{in} - \frac{t_c}{2} \right] [1 + H_d] \qquad (12)$$

where $H_d = 2e^{\left(\frac{K_0 \cdot T_2 - \frac{t_c}{2}}{(1-K_0) \cdot T_2} \right)}$.

[3] where K_0 is a positive real number smaller than 1

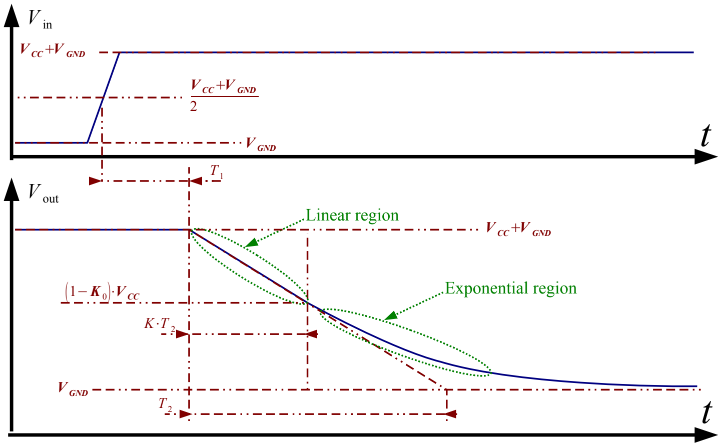

Fig. 8. Response of an ideal noise-free inverter to a step function

B Proofs

In this section, we give proofs of Lemma 1, Proposition 1 and Proposition 2.

Proof of Lemma 1 *In a neighborhood of $\overline{t_a}$, $f(t)$ can be approximated by its tangent line at time $\overline{t_a}$, giving the relation $T_a - \overline{t_a} = \frac{n(\overline{t_a})}{f'(\overline{t_a})}$. Since $n(\overline{t_a}) \sim \mathcal{N}(0, \sigma^2)$, $T_a \sim \mathcal{N}\left(\overline{t_a}, \frac{\sigma^2}{f'(\overline{t_a})^2}\right)$. The same holds for T_b in a neighborhood of $\overline{t_b}$, because $n(t)$ is stationnary. By its definition, $P_{out} = T_b - T_a$. If T_a and T_b are independent, P_{out} follows a normal distribution with mean $\mu_{out} = \overline{t_b} - \overline{t_a} = \frac{t_c}{2} + \left[p_{in} - \frac{t_c}{2}\right][1 + H_d]$ from Appendix A and variance $\sigma^2_{out} = \sigma^2_{T_b} + \sigma^2_{T_a} = \sigma^2 \left(\frac{1}{f'(\overline{t_a})^2} + \frac{1}{f'(\overline{t_b})^2}\right)$.*

Proof of Proposition 1 *(by recurrence on N)*
Lemma 1 gives expression of μ_{out_N} and $\sigma^2_{out_N}$ for $N = 1$. Let $\{I_j\}_{j=1\dots N+1}$ be a set of inverters and let V_N be the signal between the two last inverters. Logically, output of inverter I_N becomes intput of inverter I_{N+1}. Let V_{in} be the input signal of the first inverter I_1 and V_{out} is the output signal of last inverter I_{N+1} in the chain. p_{in} is the length of a pulse at I_1. Let P_N be the length of the corresponding pulse appearing at signal V_N and P_{N+1} be the length of the pulse at V_{N+1}. By assumption of reccurence,

$$P_N \sim \mathcal{N}(\mu_{out_N}, \sigma^2_{out_N}) \textit{ with } \begin{cases} \mu_{out_N} = \frac{t_c}{2} + \left(p_{in} - \frac{t_c}{2}\right)(1 + H_d)^N \\ \sigma^2_{out_N} = \sigma^2_{out}\left(\frac{(1+H_d)^{2N}-1}{(1+H_d)^2-1}\right) \end{cases}$$

According to Lemma 1, $P_{N+1} \sim \mathcal{N}(\mu_{out}, \sigma^2_{out})$ with $\mu_{out} = \frac{t_c}{2} + \left(p_n - \frac{t_c}{2}\right)(1 + H_d)$ where p_n is a realization of P_N. Assuming independence of noise sources in the chain, we have

$\mu_{out_{N+1}} = \frac{t_c}{2} + \left(\mu_{out_N} - \frac{t_c}{2}\right)(1+H_d)$ *and* $\sigma^2_{out_{N+1}} = \sigma^2_{out_N}(1+H_d)^2 + \sigma^2_{out}$ *giving*

$$\mu_{out_{N+1}} = \frac{t_c}{2} + \left(\frac{t_c}{2} + (p_{in} - \frac{t_c}{2})(1+H_d)^N - \frac{t_c}{2}\right)(1+H_d) = \frac{t_c}{2} + \left(p_{in} - \frac{t_c}{2}\right)(1+H_d)^{N+1}$$

and $\sigma^2_{out_{N+1}} = \sigma^2_{out}\left(\frac{(1+H_d)^{2N}-1}{(1+H_d)^2-1}\right)(1+H_d)^2 + \sigma^2_{out} = \sigma^2_{out}\left(\frac{(1+H_d)^{2N+2}-(1+H_d)^2}{(1+H_d)^2-1} + 1\right) = \sigma^2_{out}\left(\frac{(1+H_d)^{2N+2}-1}{(1+H_d)^2-1}\right)$.
The statement in Proposition 1 is true for $N+1$. *By recurrence over* N, *Proposition 1 is true for any* N.

Proof of Proposition 2 *We propose the proof for* PL_S *(the same is valid for* PK_S *by replacing* τ_1 *with* τ_2*).*
Assuming that there is a pulse pl_{S-1} *at* V_L, *the corresponding pulse* PL_S *at* V_L *after crossing the branches* K *and* L *(equivalent to a single chain of* $4M+2$ *inverters) is given as follows (according to Proposition 1 with* $N = 4M+2$*):*

$$PL_S \sim \mathcal{N}\left(\frac{t_c}{2} + \left(pl_{S-1} - \frac{t_c}{2}\right)R,\ \underbrace{\sigma^2_{out}\left(\frac{R^2-1}{(1+H_d)^2-1}\right)}_{\sigma^2_{out_{4M+2}}}\right),$$

where $R = (1+H_d)^{4M+2}$ *and* $t_c = \tau_1 + \tau_2$.
Thus, assuming independence of noise sources in chains K *and* L, *we have two relations of reccurence on* $\mu_{L_S} = \frac{\tau_1+\tau_2}{2} + \left(\mu_{L_{S-1}} - \frac{\tau_1+\tau_2}{2}\right)R$ *and on* $\sigma^2_{L_S} = \sigma_{out^2_{4M+2}} + \sigma^2_{L_{S-1}}R^2$.
It is easy to show that $\forall S \geq 1$,

$$\mu_{L_S} = \frac{\tau_1+\tau_2}{2} + (\mu_{L_0} - \frac{\tau_1+\tau_2}{2})R^S = \frac{\tau_1+\tau_2}{2} + \frac{\tau_1-\tau_1}{2}R^S,$$
$$\sigma^2_{L_S} = R^{2S}\sigma^2_{L_0} + \sigma^2_{out_{4M+2}}\sum_{i=0}^{S-1}(R^2)^i = R^{2S}\sigma^2_{out_{2M+1}} + \sigma^2_{out_{4M+2}}\frac{R^{2S}-1}{R^2-1}.$$

According to Proposition 1,
$\sigma^2_{out_{2M+1}} = \sigma^2_{out}\frac{(1+H_d)^{4M+2}-1}{(1+H_d)^2-1} = \sigma^2_{out}\frac{R-1}{(1+H_d)^2-1}$ *and* $\sigma_{out_{4M+2}} = \sigma^2_{out}\frac{((1+H_d)^{4M+2})^2-1}{(1+H_d)^2-1} = \sigma^2_{out}\frac{R^2-1}{(1+H_d)^2-1}$,
therefore $\sigma^2_{L_S} = \sigma^2_{out}\frac{R^{2S+1}-1}{(1+H_d)^2-1}$.