Impact of Process Mismatch and Device Aging on SR-Latch Based True Random Number Generators

Javad Bahrami[1], Mohammad Ebrahimabadi[1](✉), Sylvain Guilley[2,3], Jean-Luc Danger[3], and Naghmeh Karimi[1]

[1] University of Maryland Baltimore County, Baltimore, MD, USA
e127@umbc.edu
[2] Secure-IC S.A.S., Cesson-Sévigné, France
[3] LTCI, Télécom Paris, Institut Polytechnique de Paris, Palaiseau, France

Abstract. The True Random Number Generator (TRNG) is an inescapable primitive for security and cryptographic functions. A common TRNG architecture in digital devices exploits the noise jitter accumulation with ring oscillators. The Set-Reset latch (SR-latch) TRNG is another type which exploits the state of latches around metastability. In this TRNG the dynamic noise is extracted by analysing the convergence state of the related latch. The advantage is its very high throughput as it runs at (or near) the clock frequency. However, it is not so popular as there is no assurance that the quality of the randomness will exist in real silicon. This notably comes from the fact that there is a lack of a proven stochastic model against the quality of the process, and about its unknown behavior evolution over time (when aged). This makes the evaluation methods, like BSI AIS-31 or NIST SP 800-90B, difficult to succeed. To fill the gap, in this paper, we propose a closed form of the average entropy of the SR-latch based TRNG taking into account the process mismatch and allowing the designer to know precisely the number of SR-latches required for an optimal entropy. This is highly crucial to avoid low entropy if not enough latches are integrated, yet meanwhile preventing high overhead by not including more latches than needed. Moreover, the impact of device aging is deeply studied by simulation over 7 years. Interestingly, the results show that the aging has no significant impact on the entropy. This makes the SR-latch based TRNG a good candidate, for main TRNG or as a second entropy source.

Keywords: SR-latch based TRNG · stochastic model · regulatory standards · number of instances for a given entropy goal · impact of aging · self-rejuvenation of SR-latch TRNG

1 Introduction

Context. The generation of random numbers is essential to execute cryptographic protocols. More precisely there is a strong requirement to use a "true"

R. Wacquez and N. Homma (Eds.): COSADE 2024, LNCS 14595, pp. 177–196, 2024.
https://doi.org/10.1007/978-3-031-57543-3_10

random number generator (TRNG) which exploits physical sources and is nondeterministic, contrary to “pseudo” random number generators which are derived from mathematical sequences. For instance, initialization vectors of AES operating modes, HMAC keys, ECDSA nonces, Crystals Kyber noise, masking of protected implementations, etc. all need to be provided by TRNGs. Hence, TRNGs in CMOS digital devices have been put forward.

Ring-Oscillator based TRNGs (RO-TRNG [1]) have been studied for a while and their security level is well known [2]. As they rely on the accumulation of jitter at each ring oscillation, their throughput is limited to a few dozen of Mb/s. Moreover, leveraging only one type of TRNG exposes the risk of *single point of failures* (SPOFs) which can wreck havoc the entire system, for lack or loss of entropy (see e.g., [3,4]).

Our Subject-Matter: The SR-Latch Based TRNG. To fill the gap, in this paper we tackle another type of TRNG entropy source relying on a bistable element: the so-called Set-Reset latch (SR-latch). Contrary to the Ring Oscillator which exploits the phase noise of a free-running combinational loop, the bistable latch exploits the amplitude noise when it is near its metastable state, i.e., between the two stable states ‘0’ and ‘1’ where a small dynamic noise forces the latch to go to a stable state. Thus, the latch plays both the role of *amplifier* and *extractor* of the physical noise to the digital domain. Such an entropy source is particularly fast as it can run at a very high speed rate. This type of entropy source is already used in the Intel’s Ivy bridge [5] which is a full custom and analog technology. However, it requires a lot of care at the design stage as starting in a metastable state is hardly possible and a smart feedback loop is necessary to remain metastable. More importantly, it is not portable to any CMOS digital technology.

Problematic. In CMOS devices, an approach to use SR-latch based TRNG is to use a set of latches as proposed in [6–9]. However, this fully digital approach is not without risk, as there is no proven assurance that the entropy will be satisfactory in silicon, which is sensitive to process mismatch. Moreover, the impact of device aging has to be known to make sure the entropy is not going down over time [10]. Our first approach to assess the SR-latch TRNG was initiated in [11], yet that research provided neither a formal and in-depth study in investigating the number of latches needed for the SR-Latch TRNG nor a thorough analysis of the impact of aging on this type of TRNG. To fill the gap, this paper aims at formalizing and validating the TRNG relying on SR-latches against the process mismatch and device aging.

Our Contributions. More precisely the contributions of this paper are:

1. Proof of the scholastic model of the SR-latch TRNG to formalize the average entropy against the process mismatch;
2. Study of the impact of device aging on the SR-latch based TRNGs;
3. Demonstration that the mean entropy of a batch of SR-latch based TRNGs is not significantly impacted when aging.

Outline. The rest of this paper is organized as follows. After presenting the background in Sect. 2, Sect. 3 formalizes the proof expressing the stochastic model of entropy against the mismatch. Section 4 deals with the impact of aging on the targeted TRNGs and Sect. 5 discusses the experimental results. Finally, Sect. 6 concludes the paper and draws future directions of this research.

2 Research Background

2.1 SR-Latch Based TRNG

TRNGs in digital devices leverage clock jitter noise or the noise around metastable states for generating random numbers. While oscillator-based TRNGs (e.g., RO-based or self-timed rings [12]) are robust, metastable-state based TRNGs offer speed advantages. However, benefiting from metastable states is more tricky as it requires analog and custom cell design [5,13]. To tackle such a problem in a fully digital environment, deploying SR-latches has been proposed in the literature [6].

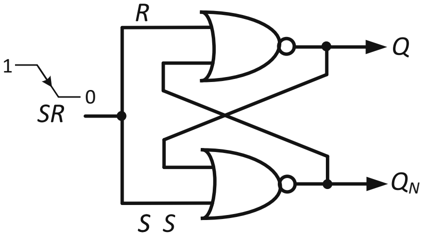


Fig. 1. An SR-latch realized via cross-coupled NOR gates.

Figure 1 depicts a NOR-based SR-latch TRNG. The Set (S) and Reset (R) inputs are both derived from the same SR signal. With perfectly balanced NOR gates, the latch enters a metastable state at around $V_{dd}/2$ voltage when SR goes to zero. Then the dynamic environmental noise pushes the latch to a stable state V_{dd} (logic '1') or logic '0', hence creating an entropy extractor from the physical noise to the digital world. Figure 2 depicts the simulations of this latch for $V_{dd} = 1.2$ V and a temperature of 25 °C. The simulation is a *transient noise analysis* for 100 cycles with a noise of min/max frequency equal to 10 kHz/20 GHz. The simulation engine is `Spectre`, running on the placed-and-routed netlists where parasitics had been extracted by `Innovus`, both tools being commercialized by Cadence. As shown, the propagation time between SR and Q or Q_N depends on the noise magnitude when SR goes to '0'. A long propagation time should correspond to a state very near metastability. Being around the metastable state provides an optimal entropy for a small level of noise. To characterize this propagation time according to the metastability level, we consider a perfect SR-latch with two separated S and R inputs having a small time difference. This difference expresses the dynamic noise, but it can also come from a bias due to the process mismatch, which is bad for entropy as it is static. Figure 3 shows the relationship between the propagation time and this S-R time difference. As shown in this figure when there is no time difference between S and R signals, the propagation time is very high due to the metastability, yet the propagation time decreases when there is a time difference between the S and R signals.

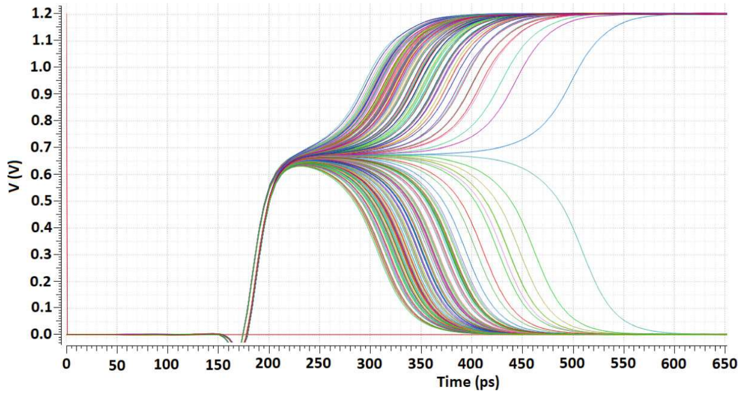


Fig. 2. Transition from a metastable to a stable state due to input noise.

By feeding SR with a periodic signal (e.g., one clock) this design yields a random bit every clock cycle, combining speed and compactness; thus efficient in terms of Power-Performance-Area (PPA).

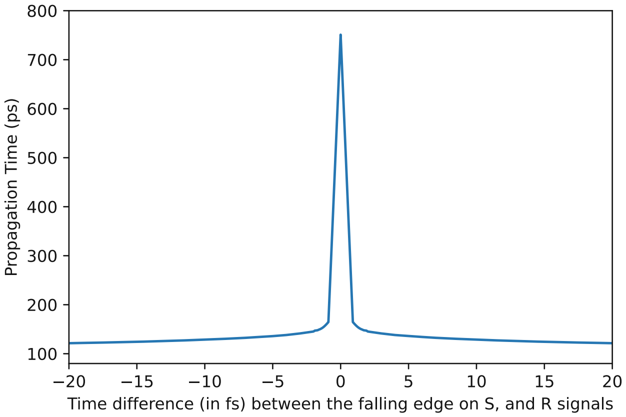


Fig. 3. Evolution of propagation time in one SR-latch based on the time difference between the falling edges on S and R signals.

The SR-latch can serve as a TRNG thanks to the dynamic noise. One first precondition is however that the routing is symmetric, if not *geometrically* at least *from the timing standpoint*. This could be achieved thanks to either *manual placement-and-routing* or *timing constraints* (e.g., SDC files). SDC constraints for balancing paths are described in [14]. The idea is to leverage a "Local Clock Set" (LCS) methodology where the SR source signal is defined as a virtual clock and S and R are set at leaves. The SDC constraint ensures that source-to-destination delays are equal, up to a bounded skew. In particular, the two NOR gates interfaces shall be plugged alike, namely input A (resp. B) receiving R (resp. Q_N) in the upper gate shall receive S (resp. Q) in the lower gate. A second precondition for the SR-latch to behave as a TRNG is that both NOR gates should be balanced, which is rarely the case as the 2 NORs are impacted by local process mismatch. Hence, the latch becomes deterministic, resembling a Physically Unclonable Function (PUF [15]). Accordingly, if multiple latches are XORed as shown in Fig. 4, we can expect that statistically a few latches will be sufficiently near metastability to provide a good entropy. This paper aims to size theoretically the number of required latches according to the mismatch and the noise level.

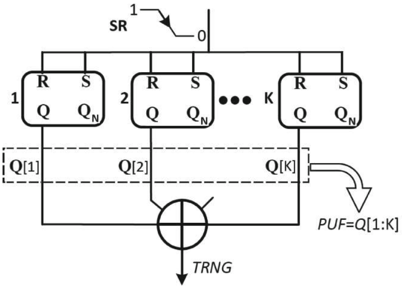


Fig. 4. The PUF-TRNG circuitry composing of a set of SR-latches.

2.2 Long-Lasting Randomness Provision

To ensure that SR-latch based TRNGs are promising for industrial applications we need to investigate their functionality over the course of usage. Indeed as the electrical specifications of transistors and in turn their delay and power consumption change over time due to device-aging [16], it is highly crucial to investigate whether a TRNG delivers high entropy even after aging or not.

In this paper, we focus on the impact of Bias Temperature Instability (BTI) and Hot Carrier Injection (HCI) [17] which are the most prominent aging mechanisms [18]. BTI includes NBTI and PBTI mechanisms (referring to negative and positive BTIs respectively) which affect PMOS and NMOS transistors respectively; resulting in the increase of their threshold voltage (Vth) when a transistor is ON. When OFF, the transistor experiences a partial recovery from the BTI stress as a result of which the aging-induced increase of its Vth partially decreases. HCI affects NMOS transistors when they experience a switching in their gate input.

This results in the change of Vth and the current passes through the transistor. Such changes increase the delay of the underlying gate during the course of usage.

3 Impact of Mismatch on the SR-Latch Based TRNG Architecture

In this section, we focus on the SR-latch based TRNGs realized via cross-coupled NOR gates unless otherwise mentioned. The NAND-based structures follow the same discussions and thus are not discussed here to prevent redundancy.

In a SR-latch based TRNG with multiple latches, each latch i has a probability of p_i to be at '1' after SR goes from '1' to '0':

$$p_i = \mathbb{P}[latch_i = 1] \, .$$

The probability p_i has to be as close as possible to the metastable state corresponding to $p_i = 1/2$. We define the bias $\varepsilon_i = p_i - 1/2$. By applying the *piling-up lemma* [19], the probabilities $P_0 = \mathbb{P}[TRNG = 0]$ and $P_1 = \mathbb{P}[TRNG = 1]$ of the $TRNG$ composed by XORing N latches are equal to:

$$P_0 = 1/2 + 2^{N-1} \prod_{i=1}^{N} \varepsilon_i, \quad P_1 = 1 - P_0 = 1/2 - 2^{N-1} \prod_{i=1}^{N} \varepsilon_i \; . \tag{1}$$

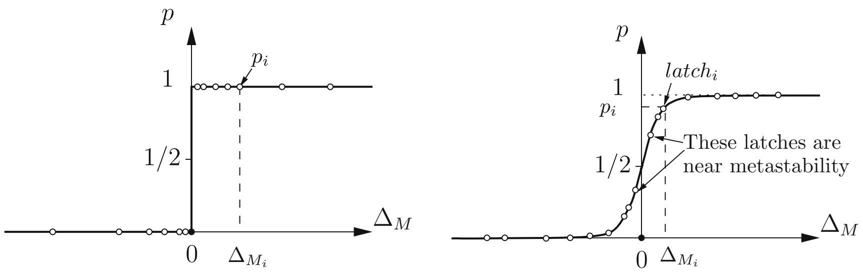
The Shannon entropy H of the TRNG, with probabilities P_0 and P_1, is given by:

$$H = -P_0 \log(P_0) - P_1 \log(P_1) \; . \tag{2}$$

The entropy equation shows that it depends only on the magnitude of the final bias $|\epsilon| = |\prod_{i=1}^{N} \varepsilon_i|$ as $H_\epsilon = H_{-\epsilon}$. The constant ϵ must be as close to zero as possible to achieve a probability near 1/2 and an optimal entropy of 1 Shannon bit. Hence, only one latch being in a metastable state (i.e., $\varepsilon_i = 0$) is enough to have an optimal entropy.

The probability p_i highly depends on the internal process mismatch between identical elements of the microelectronics process. The mismatch arises from factors such as transistor channel width/length change owing to its atomic scale [20], or doping density in the active area, where the discrete number of dopants can depend from transistor to transistor [21].

The mismatch between two NOR gates of the SR-latch i can be modeled by a delay offset Δ_{M_i} of S against R with a perfectly balanced SR-latch. For a given latch i, its output is equiprobable (i.e. $p_i = 1/2$) if the mismatch Δ_{M_i} is exactly equal to zero. Without noise, as shown in Fig. 5a, there is no chance to get this condition. With noise, the p_i of some latches with small Δ_{M_i} can be closer to 1/2; thus giving rise to the TRNG's randomness, as shown in Fig. 5b. In fully digital technology, if we consider a TRNG built by XORing multiple latches, we could think some of them could be sufficiently close to metastability to build a good TRNG. We consider that every latch has a static process mismatch Δ_{M_i} which follows a normal distribution: $\Delta_{M_i} \sim \mathcal{N}(0, \Sigma^2)$.



(a) without dynamic noise.

(b) with dynamic noise.

Fig. 5. The latches can produce entropy if $0 < p_i < 1 \implies \Delta_{M_i} = 0$ with noise.

The TRNG can be generated as there is a physical random source of dynamic noise Z considered as Gaussian: $Z \sim \mathcal{N}(0, \sigma^2)$. As expressed in Eqs. 1 and 2, the TRNG's randomness depends on the small values of the bias $\varepsilon_i = p_i - 1/2$.

To get a closed form of the entropy, let us first define the "Mismatch to Noise Ratio" MNR as being:

$$\mathsf{MNR} = \frac{\Sigma}{\sigma} . \qquad (3)$$

Intuitively, the smaller MNR, the larger the entropy.

The blue curve in Fig. 6 represents the distribution ΔM of all the ΔM_i, where ΔM_i is the process mismatch of latch i. The orange curve depicts the distribution of the measurement of ΔM_i where the Gaussian noise Z is added to ΔM_i. In this figure, the probability p_i of the latch i at '1' corresponds to the hatched area of Fig. 6.

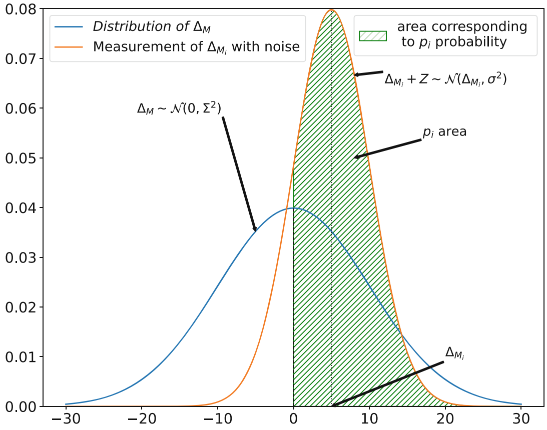


Fig. 6. Graphical representation of the probability p_i. (Color figure online)

As mentioned earlier, the entropy depends on the bias magnitude $|\prod_{i=1}^{N} \varepsilon_i|$. A closed form of the mean entropy can be obtained if we consider each latch independent from the others. This assumption is realistic since technological dispersion is very local as shown in [20,21]. In this case the mean value of the bias $\widehat{|\prod_{i=1}^{N} \varepsilon_i|} = \prod_{i=1}^{N} \widehat{|\varepsilon_i|}$.

To be exact, [20,21] focus on process-mismatch (local variation) rather than the entire process variation and noise. Hence, real measurements are crucial for understanding true dependencies. As the SR-latch structure is very close to the SRAM point (two inverters vs two gates), SRAM measurements used for PUF [22] show that the bias is limited and the probabilities are balanced for SRAM.

Lemma 1. *The mean bias* $\widehat{|\varepsilon_i|} = \widehat{|p_i - 1/2|}$ *according to* MNR *is given by:*

$$\widehat{|\varepsilon_i|} = \frac{1}{\pi} \arctan\left(\mathsf{MNR}\right). \tag{4}$$

Proof.

$$\begin{aligned} &\varepsilon_i = p_i - 1/2 \\ \implies &|\varepsilon_i| = \begin{cases} p_i - 1/2 & \text{if } p_i > 1/2 \\ 1/2 - p_i & \text{otherwise.} \end{cases} \end{aligned}$$

As p_i is equally distributed around 1/2, the mean value $\widehat{|\varepsilon_i|}$ of ε_i can be expressed as:

$$\begin{aligned} \widehat{|\varepsilon_i|} &= \widehat{p_i} - 1/2, p_i > 1/2 \\ &= \mathbb{P}\left[(\Delta_{M_i} + Z) > 0, \Delta_{M_i} > 0\right] - 1/2 \\ &= \mathbb{P}\left[\Delta_{M_i} > -Z, \Delta_{M_i} > 0\right] - 1/2 \\ &= \mathbb{P}\left[\frac{\Delta_{M_i}}{\Sigma} \cdot \mathsf{MNR} > -\frac{Z}{\sigma}, \Delta_{M_i} > 0\right] - 1/2\,. \end{aligned}$$

If we consider the variables $X = \frac{\Delta_{M_i}}{\Sigma}$ and $Y = \frac{Z}{\sigma}$, X and Y are independent and follow standard normal distributions. The formula becomes:

$$\widehat{|\varepsilon_i|} = \mathbb{P}[X \cdot \mathsf{MNR} > -Y, X > 0] - 1/2 = \mathbb{P}[Y > -X \cdot \mathsf{MNR}, X > 0] - 1/2\,.$$

Since the probability distribution of (X, Y) is isotropic, the value $\mathbb{P}[Y > -X \cdot \mathsf{MNR}, X > 0]$ when $X > 0$ equals the proportion of the grey area on Fig. 7 on the half circle when X, Y are in polar representation. This proportion is $(\theta + \pi/2)/\pi$, where $\tan(\theta) = \mathsf{MNR}$. Thus, we have:

$$\widehat{|\varepsilon_i|} = \frac{1}{\pi} \arctan\left(\mathsf{MNR}\right).$$

□

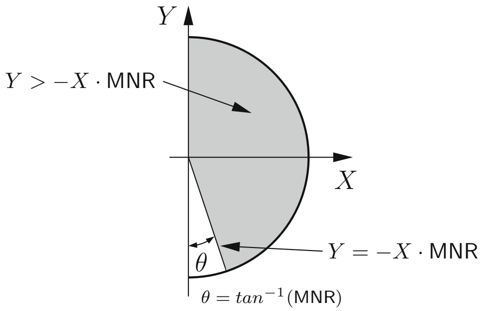

Y
$Y > -X \cdot \mathsf{MNR}$
X
θ
$Y = -X \cdot \mathsf{MNR}$
$\theta = tan^{-1}(\mathsf{MNR})$

Fig. 7. Polar representation of X and Y.

The mean probabilities $\widehat{P_0}$ and $\widehat{P_1}$ are given by Eq. 5, with $s = sign(\prod_{i=1}^{N} \varepsilon_i)$:

$$\widehat{P_0} = 1/2 + (-1)^s \cdot 2^{N-1} \left(\frac{1}{\pi} \arctan(\mathsf{MNR}) \right)^N, \quad \widehat{P_1} = 1 - \widehat{P_0} \,. \tag{5}$$

The mean entropy $\widehat{H}$ is deduced from these formulas and illustrated in Figure 8 according to the number of latches and the MNR parameter.

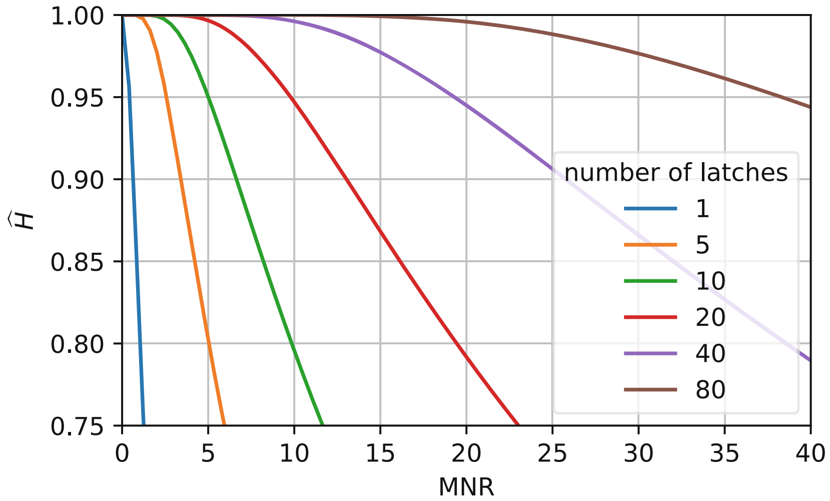


Fig. 8. Mean Entropy $\widehat{H}$ according to Mismatch to Noise Ratio (MNR) for different number of latches.

In the study presented in [9] about SR-latch in FD-SOI 28 nm technology, the MNR was estimated at 7. For such MNR value, Fig. 8 indicates that at least 40 SR-latches are necessary to have an average entropy of 1 bit. More precisely, with 40 SR-latches, the entropy is greater than 0.997 bit, which is the threshold value mandated by the AIS-31 standard [2]. In this research, we characterize Σ by the sweeping method, which will be introduced in Sect. 5.2. Meanwhile we add artificial noise to SR signals to find the number of required latches based on Fig. 8. Note that the impact of routing/parasitics can be modeled by adding safety margins in the number of latches.

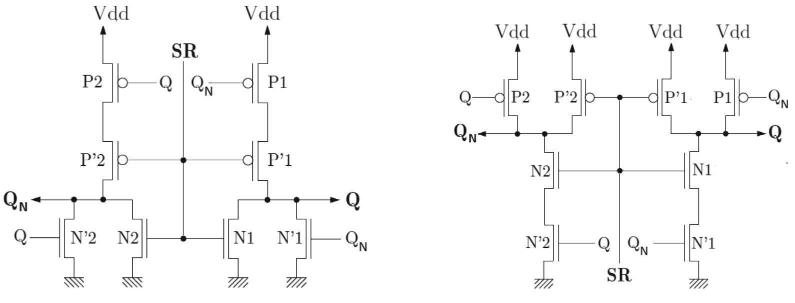
4 Impact of Aging on the SR-Latch Based TRNG

As BTI impact is more prominent than HCI and other aging mechanisms, we focus on the BTI aging in our analysis in this section. We can simplify the conditions in which the BTI aging occurs with the following rules which correspond to the conduction of the transistor:

- A PMOS is degraded (in terms of stress resulting in the increase of its threshold voltage and in turn its delay) by NBTI aging when gate = '0', source = '1' (and thus drain = '1');
- An NMOS is degraded by PBTI aging (in terms of stress) when its gate = '1', source = '0' (and thus the drain = 0).

In this section, we discuss the impact of aging on both NOR- and NAND-based TRNGs for the sake of completeness, yet as both structures behave similarly, for the sake of space, we focus only on the NOR-based structures in Sect. 5 where we present the experimental results.

4.1 Aging Analysis for NOR-Based SR-Latch



(a) NOR-based TRNG.

(b) NAND-based TRNG.

Fig. 9. Structures of the NOR and NAND SR-latch based TRNGs.

Here we focus on the TRNG structure realized with NOR-based SR-latches shown in Fig. 9a. In the initial phase SR is '1' and so the output of each NOR becomes '0'. Without loss of generality, let's assume that the output Q_N changes faster than Q (due to mismatch). In this case when SR goes from '1' to '0', the output Q_N rises faster than Q and toggles to '1', whereas Q stays at '0'. Therefore in such a situation the transistors' aging would be as below:

- When SR = 1 $\implies$ N1, N2, P1, P2 get aged;
- When SR = 0 $\implies$ N'1, P2, P'2 get aged;
- N'2 and P'1 do not get aged.

The above discussion shows that P2 almost ages twice more than P1. Also P'2 ages more than P'1. This should slow down Q_N. *This analysis shows that aging can have a positive impact towards metastability on this latch as Q_N changes slower than Qdue to aging (referring to the above discussion) while it was faster initially.*

To support our analysis, we have conducted HSpice simulations and extracted the aging impacts in terms of the evolution of Vth over 7 years of usage (with the steps of 2 months) for the NOR-based SR-latch in Fig. 9a. The results depicted in Fig. 10 follow our above discussion. For example, as shown the change of Vth in P2 increases is almost twice more than P'2. Also please note that NBTI impact (in PMOS transistors) is almost twice of PBTI impact in NMOS transistors.

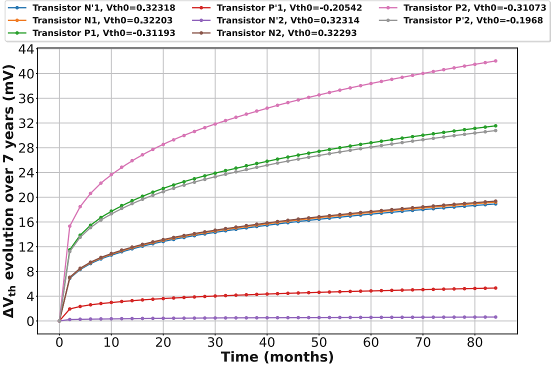


Fig. 10. Threshold voltage (Vth) evolution with aging for the NOR-based SR-latch. Vth0 denotes the initial threshold (before aging) for each transistor.

4.2 Aging Analysis in NAND-Based SR-Latch

Similar to the NOR-based SR-latch discussed earlier, in this section we analyze the aging impact in the NAND-based structure shown in Fig. 9b. In this structure, initially we give '0' to SR and so the output of each NAND would be '1'. Without loss of generality, here we assume that the output Q is changed faster than Q_N when going from the initial to final phase, i.e., when SR goes from '0' to '1', the output Q will fall faster than Q_N and thus Q toggles to '0', whereas Q_N stays at '1' and loses the race. Therefore in such situation the transistors aging would be as follows:

- When SR = 0 $\implies$ N'1, N'2, P'1, P'2 get aged;
- When SR = 1 $\implies$ N'1, N1, P2 get aged;
- N2 and P1 do not get aged.

The above discussion shows that N'1 ages almost twice more than N'2 and N1 while N2 does not age much (unless for HCI). Thus the change of Q gets slow over the course of usage (aging) although it was faster initially compared to Q_N. *This again confirms that aging can positively affect the TRNG over time and results in metastability and thus higher randomness.*

Our HSpice simulation result for the NAND-based Latch is shown in Fig. 11 which again follows our above discussion. For example as shown N'1 ages twice more than N1. Note that in Fig. 10 and Fig. 11 the graphs depicting the ΔVth have overlap for some transistors and may not be seen clearly (e.g., N1 and N'1 in Fig. 10). Also it is noteworthy to mention that NBTI effect (as expected) is more than PBTI thus the PMOS transistors observe more change in their threshold voltage than the NMOS counterparts in similar situations (i.e., being ON for the same amount of time).

In sum, the above analysis and the extracted results can lead to the conclusion that aging can move the SR-latch based TRNG towards more metastability for both NOR and NAND based circuits. Albeit there are some high-order effects which make the analysis of the SR-latch based TRNGs not straightforward. Accordingly, experimental results with electrical simulation are necessary to better learn the impact of aging on the SR-latch TRNGs. We will show such results in the next section.

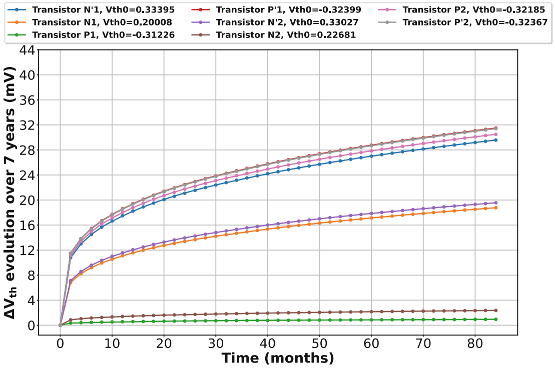


Fig. 11. Threshold voltage (Vth) evolution with aging for the NAND-based SR-latch. Vth0 denotes the initial threshold (before aging) for each transistor.

5 Experimental Results and Discussions

5.1 Experimental Setup

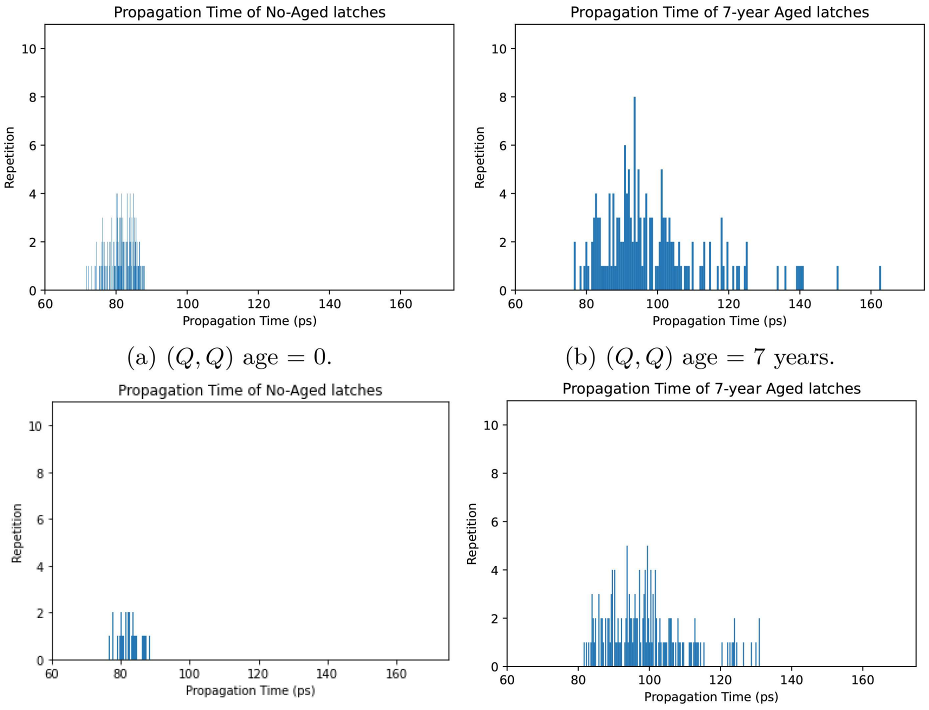
We implemented the TRNGs at the transistor level using a 45nm open-source NANGATE library [23]. Our Initial netlist includes 1024 SR-latches in parallel (recall Fig. 4). To mimic the real-silicon behavior, we considered process mismatch through Monte-Carlo simulations with Gaussian distributions: transistor gate length L: $3\sigma = 10\%$, threshold voltage V_{th}: $3\sigma = 30\%$, and gate-oxide thickness t_{OX}: $3\sigma = 3\%$. This allows us to derive the delay offset of the mismatch Δ_M through the sweeping process that will be discussed in the next section. Moreover to resemble real silicon, we also added a white noise to the input of each latch with $\mu = 0$ and $\sigma = 1.029$ ps.

In our implementation of the SR-latch based TRNG, while the Q_N outputs of all latches are left floating, the Q outputs are XORed to build the final single bit of randomness. Also, We added buffers on SR signals to include the inputs' slope (between 81.43V/ps and 99.65V/ps for the smallest and largest buffers, respectively) however this did not highly affect TRNG's metastability. We used Synopsys HSpice for the simulations, and the HSpice built-in MOSRA Level 3 model [24] to evaluate aging effects for 7 years of device operation in different time steps from minutes (30 min) to months (6 months). We considered BTI and HCI for aging simulations, however we just discussed NBTI for the 1^{st}-order analysis in our discussion. The simulations were conducted for the temperature of 85°C, $V_{dd} = 1.2$ V.

5.2 Experimental Results

A. Impact of Aging on the Propagation Time of the TRNG: The first set of results relates to the propagation time of the latches composing a TRNG considering their metastability status. Indeed, as discussed in Sect. 2, propagation time significantly increases when approaching metastability as shown in Fig. 3. To measure the propagation time of each underlying latch, we applied a falling edge signal to both R and S of the latch and kept the SR (the signal feeding both S and R) value '0' till either Q or Q_N get stable at '1'. The propagation time is defined as the time difference from when the SR signal crosses 0.8 V until the absolute value of $Q - Q_N$ exceeds 0.8 V. To analyze the results, we categorized the latches into 2 sets based on their outcome. In the first set, the outputs of latches stay at the same value, e.g, $(Q, Q_N) = (1, 0)$ when SR goes to 0 without aging and stay at $(1, 0)$ after aging. For the second set, the output toggles with aging: $(Q, Q_N) = (1, 0) \Rightarrow (Q, Q_N) = (0, 1)$ and vice-versa.

SR-Latches Keeping the Same State: Figures 12a and 12b illustrate the histogram of propagation time for latches keeping the state $Q = 1$ in both new and 7 years-aged latches. As depicted, aging increases the propagation time; with averages of 81.63 ps for new latches and 98.87 ps for aged latches. A similar observation can be made for latches staying with state $Q_N = 1$ in Figs. 12c and 12d, with the average propagation time increasing from 82.4 ps to 99.35 ps. This implies that for this first set of latches which keep the same state for both fresh and aged devices, there is a trend to go towards metastability, thus corroborating the analysis in Sect. 4. This should improve the quality of the TRNG over time. To investigate the aging impacts on the SR-latch in more detail, the evolution of the propagation time when the SR-latches are aged is shown for different aging steps. Figure 13a and Fig. 13b depict the cases for two sample latches (among the 1024 latches we simulated) whose output stays at $Q = 1$ before and during the



(a) (Q, Q) age = 0.

(b) (Q, Q) age = 7 years.

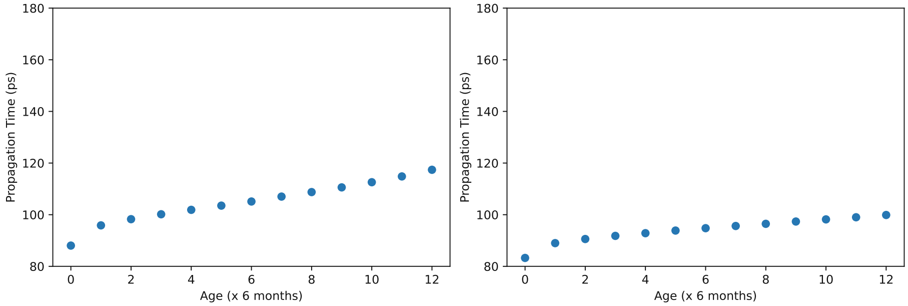
(c) (Q_N, Q_N) age = 0.

(d) (Q_N, Q_N) age = 7 years.

Fig. 12. Distribution of the propagation time of the SR-latch when the fresh and aged devices have the same state.

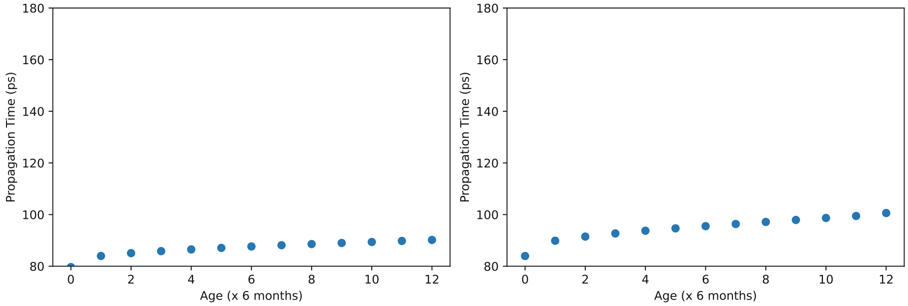
course of aging. We can notice that the propagation time increases monotonically but not at the same rate. We observe the same effect for latches whose output stays at $Q_N = 1$ as shown in Fig. 14a and Fig. 14b. This monotonic evolution of the propagation time is not the same for all the latches but all go toward the metastable state, thus involving a better entropy.

SR-Latches with State Toggling: For this second set of latches, the outputs change state with aging. If the no-aged SR-latch outputs $(Q, Q_N) = (1, 0)$ after SR goes to 0, when it changes to $(0, 1)$ after a certain amount of age. The propagation time starts to increase, as expected according to the analysis of Sect. 4, but decreases once the state goes beyond metastability, involving a toggling of the output. This is illustrated in Fig. 15 where we can observe the toggling on their output in a different port after some time of aging. As shown, the propagation time increases first but after such toggling at time t it starts decreasing. For example, for the first sampled latch in Fig. 15a such toggling occurs after $t = 180$ min $(= 6 \times 30)$ of aging. For the other samples, as shown in Fig. 15b-15c-15d, the toggling occurs at a different point of time (42 months, 150 min and 50 days) due to the process mismatch. It is interesting to note that the mismatch



(a) (Q, Q) (b) (Q, Q)

Fig. 13. Evolution of propagation time with aging for 2 sample latches keeping the state $Q = 1$.



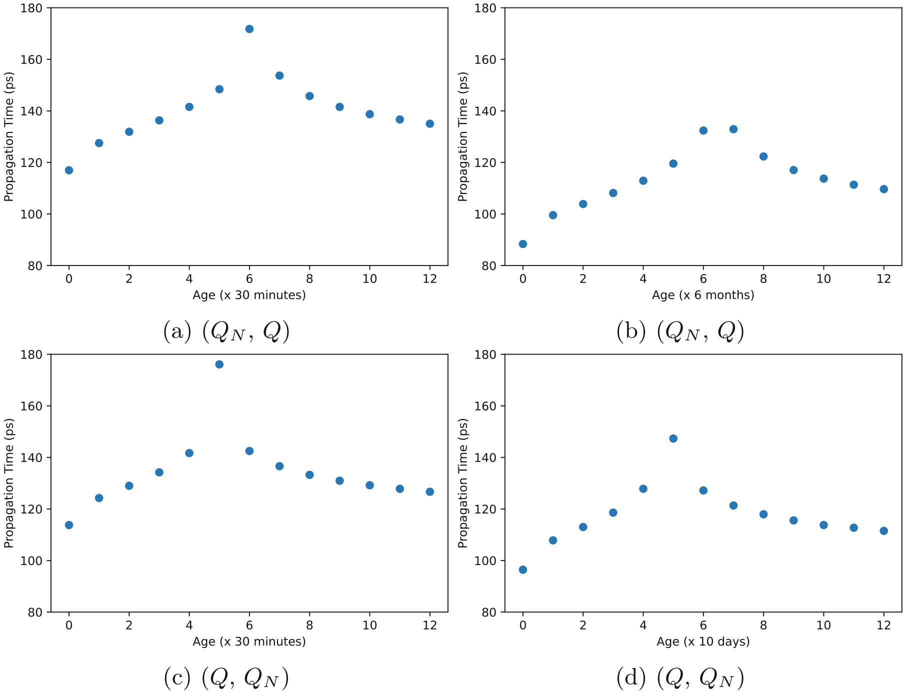
(a) (Q_N, Q_N) (b) (Q_N, Q_N)

Fig. 14. Evolution of propagation time with aging for 2 sample latches keeping the state $Q_N = 1$.

for this set of latches, expressed in the time difference between the S and R signals, is small, below 1 ps, while in other cases such difference is higher than 1.11 ps.

The takeaway from these observations is that the reasoning of Sect. 4 applies and the latches go toward the metastable state and contribute to the increase of the propagation time. However, for the set of latches that are near metastability and thus their output toggle due to the course of aging, the propagation time decreases after toggling, meaning that their state goes away from metastability. This could decrease the entropy of the SR-latch TRNG for these cases.

B. Process Mismatch Characterization and Entropy Assessment. This set of results extracts process mismatch impact in terms of their effect on the transient response time of TRNGs. This evaluation is essential in assessing the MNR value (recall Eq. 3) and in turn deciding about the number of latches to be inserted in the TRNG design for fabrication.



(a) (Q_N, Q)

(b) (Q_N, Q)

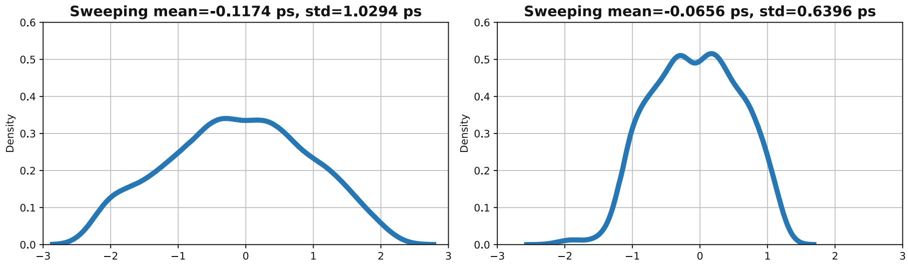
(c) (Q, Q_N)

(d) (Q, Q_N)

Fig. 15. Evolution of propagation time with aging for 2 sample latches whose outputs toggle during the aging.

In this experiment we do not add any noise to be able to see the sole impact of process mismatch among different latches and even among the 2 NOR gates resided in each latch. To do so, we inject a transition (fall in case of NOR-based latch) in S signal and then sweep the R signal such that it observes a transition in a different time. Then we measure the time difference between the transitions on S and R that results in toggling the latch output (*the time that the latch goes to its final state and exits the metastable state*). This time (referred to as ΔM_i for each latch i in Sect. 3) is changed from one latch to another due to process mismatch and manifests the impact of process mismatch in the randomness of the TRNG. In our experiments, the sweeping step is 80 fs.

Figures 16a and 16b show the distribution of the extracted ΔM_i for the NOR-based TRNGs when they are new (age = 0) or 7-year old. In this experiment, we initially inserted 1024 latches to find the MNR value and then decide about the number of latches based on Fig. 8. As expected the distributions follow a Gaussian model. When fresh (age:0), the results exhibit a mean of −0.1173 ps and a standard deviation of 1.0294 ps while the mean and standard deviation of the 7-year aged TRNGs is −0.0655 ps and 0.6396 ps, respectively. As shown through the course of aging, the standard deviation of the distribution of ΔM_i decreases. The takeaway point from these observations is that the SR-Latch



(a) age = 0

(b) age = 7 years

Fig. 16. Distribution of the ΔM_i for the targeted NOR-based TRNGs when they are new (age = 0) or 7-year old.

based TRNG becomes more metastable over time; thus its randomness increases over the course of usage. This confirms that SR-latch based TRNGs remain qualified (if not getting better) over time. In practice, the effect of temperature on the entropy of the TRNG is insignificant as temperature affects all NOR gates (or NAND gates) similarly.

In the next step, we conducted simulations to get the mean entropy for MNR = 10 and MNR = 20. As the standard deviation of the process mismatch is at $\Sigma = 1.0294$ ps in Fig. 16a), we used respectively a Gaussian noise with $\sigma =$ 100 fs and 50 fs at the input of the S signal. The entropy is calculated using Eq. 2 for a number of latches $\in \{20, 40, 80\}$. As shown in Table 1, the average entropy greatly increases with the number of latches and is slightly increased with aging but not monotonically as discussed in the next section. This is comparable with the theoretical analysis of the mean entropy in Fig. 8, especially when the number of latches increases, involving a lower statistical bias.

Table 1. Aging-induced evolution of the mean Entropy for MNR = 10 (left) and MNR = 20 (right) when we have 20, 40, and 80 latches.

#latches year	20	40	80
0	0.833	0.985	0.997
2	0.927	0.995	0.999
4	0.960	0.999	1
6	0.940	0.995	1

#latches year	20	40	80
0	0.580	0.876	0.943
2	0.700	0.918	0.995
4	0.731	0.923	0.994
6	0.721	0.913	0.999

5.3 Discussion

Here we analyze the results presented and interpret the experimental results presented earlier. Furthermore, we comment more generally on our contributions.

It is known that, in general, aging increases the variability, on individual gates. However, given the symmetrical structure of SR-latches, such variability happens to contribute to fix their structural imbalance (rooted in local technology dispersion). This is due to the fact that SR-latches are differential elements, which react according to the relative delay between S and R inputs; this delay decreases in average when variability increases. As a result, SR-latches that have initially poor entropy are likely to become more entropic after aging.

Our simulation results show that the throughput of the SR-latch based TRNG is considerably high compared to RO-based TRNG (which is around 3Mb/s per [25]). Based on our simulation with NANGATE, the throughput of SR-latch based TRNG changes from 12 Gsample/s for a new device to 10 Gsample/s after 7 years of aging.

It is also probable that some SR-latches that are well balanced at birth go further from their tiny balance after aging. However, in general, this situation is rare because only a minority of SR-latches happen to be fabricated well balanced. All in all, the mean of the entropy should slightly increase with aging.

Notice that metastability, in that a signal is not resolved, is not the phenomenon we leverage as an entropy source. Still metastability is correlated to the fact that an SR-latch is behaving randomly. In practice, anyway, the output of an SR-latch is re-sampled, resolving the metastability. Hence, we insist that in terms of the stochastic model, the entropy arises from the difference between S and R input signals.

Regarding the industrial interest in SR-latch TRNGs, one should note that they nicely complement other TRNGs designs, such as ring-oscillator TRNGs. Notice that some TRNGs have been found to fail [26]. It is thus a safe practice to implement two instances of TRNGs with different rationales. This is even mandated by regional regulations such as OSCCA GM/T-0078 in China.

Eventually, let us comment on the PPA. Our findings in Sect. 5.2 is that 80 SR-latches are required for the technology we considered, which means roughly 160 gate equivalent (GE). Such size of entropy source is very small, compared to RO-TRNG (recall that the seminal paper on the RO-TRNG [1] contender suggests 114 RO, each comprised of dozens of GE). This low overhead makes SR-latch based TRNGs even more appealing; on top of its better or at least same entropy (not less) when aged.

6 Conclusion

The study in this paper allows to better control and understand the behavior of SR-latch TRNG against the process mismatch and aging. This type of TRNG provides very high throughput compared to RO-based but is not well mastered in digital technology. The presented work paves the way towards a better comprehension of the SR-latch allowing the TRNG designer to use it in a trusted manner. The impact of mismatch has notably been formally expressed to size the number of latches according to the required entropy and the environmental noise. It is also shown that the aging provides a slight improvement towards the metastability of latches, hence a better entropy of the TRNG. Future works are to confirm these results on real devices with different process mismatch and noise levels. Another important work is to formally analyze the second order impact of aging, i.e. when the latches toggle and move away from metastability.

Acknowledgements. Secure-IC acknowledges partial funding from the European Union's Horizon Europe research and innovation program through ALLEGRO project, under grant agreement No. 101070009. This research is also supported in part by the National Science Foundation CAREER Award under Grant NSF CNS-1943224.

References

1. Sunar, B., Martin, W.J., Stinson, D.R.: A provably secure true random number generator with built-in tolerance to active attacks. IEEE Trans. Comput. **56**(1), 109–119 (2007)
2. Peter, M., Schindler, W.: A Proposal for Functionality Classes for Random Number Generators, Version 2.0 (2022). https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Certification/Interpretations/AIS_31_Functionality_classes_for_random_number_generators_e.pdf?__blob=publicationFile&v=5
3. Markettos, A.T., Moore, S.W.: The frequency injection attack on ring-oscillator-based true random number generators. In: Cryptographic Hardware and Embedded Systems (CHES), vol. 5747, pp. 317–331 (2009)
4. Martin, H., Martin-Holgado, P., Peris-Lopez, P., Morilla, Y., Entrena, L.: On the entropy of oscillator-based true random number generators under ionizing radiation. Entropy **20**(7), 513 (2018)
5. Hamburg, M., Kocher, P., Marson, M.E.: Analysis of Intel's Ivy Bridge digital random number generator (2012). http://www.cryptography.com/public/pdf/Intel_TRNG_Report_20120312.pdf
6. Danger, J.-L., Guilley, S., Hoogvorst, P.: High speed true random number generator based on open loop structures in FPGAs. Microelectron. J. **40**(11), 1650–1656 (2009)
7. Lozach, F., Ben-Romdhane, M., Graba, T., Danger, J.-L.: FPGA design of an open-loop true random number generator. In: Euromicro Conference on Digital System Design (DSD), pp. 615–622 (2013)
8. Ben-Romdhane, M., Graba, T., Danger, J.-L., Mathieu, Y.: Design methodology of an ASIC TRNG based on an open-loop delay chain. In: New Circuits and Systems Conference (NEWCAS), pp. 1–4 (2013)
9. Danger, J.-L., et al.: Analysis of mixed PUF-TRNG circuit based on SR-latches in FD-SOI technology. In: Euromicro Conference on Digital System Design (DSD), pp. 508–515 (2018)
10. Fischer, V.: A closer look at security in random number generators design. In: Constructive Side-Channel Analysis and Secure Design (COSADE), pp. 167–182 (2012)
11. Bahrami, J., Ebrahimabadi, M., Danger, J., Guilley, S., Karimi, N.: Special session: security verification & testing for SR-latch TRNGs. In: VLSI Test Symposium (VTS), pp. 1–10 (2023)
12. Cherkaoui, A., Fischer, V., Fesquet, L., Aubert, A.: A very high speed true random number generator with entropy assessment. In: Cryptographic Hardware and Embedded Systems (CHES), vol. 8086, pp. 179–196 (2013)
13. Kinniment, D., Chester, E.: Design of an on-chip random number generator using metastability. In: European Solid-State Circuits Conference, pp. 595–598 (2002)

14. Gimenez, G., Cherkaoui, A., Cogniard, G., Fesquet, L.: Static timing analysis of asynchronous bundled-data circuits. In: International Symposium on Asynchronous Circuits and Systems (ASYNC), pp. 110–118 (2018)
15. Maes, R.: Physically Unclonable Functions - Constructions, Properties and Applications. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-41395-7
16. Anik, M.T.H., Reefat, H.I., Danger, J.-L., Guilley, S., Karimi, N.: Aging-induced failure prognosis via digital sensors. In: ACM Great Lakes Symposium on VLSI (GLSVLSI), pp. 703–708 (2023)
17. Oboril, F., et al.: Extratime: modeling and analysis of wearout due to transistor aging at microarchitecture-level. In: DSN, pp. 1–12 (2012)
18. Huang, K., Anik, M.T.H., Zhang, X., Karimi, N.: Real-time IC aging prediction via on-chip sensors. In: 2021 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), pp. 13–18 (2021)
19. Matsui, M.: Linear cryptanalysis method for DES cipher. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 386–397. Springer, Heidelberg (1993). https://doi.org/10.1007/3-540-48285-7_33
20. Asenov, A., Kaya, S., Davies, J.H.: Intrinsic threshold voltage fluctuations in decanano mosfets due to local oxide thickness variations. IEEE Trans. Electron Devices **49**(1), 112–119 (2002)
21. Asenov, A., Slavcheva, G., Brown, A.R., Davies, J.H., Saini, S.: Increase in the random dopant induced threshold fluctuations and lowering in sub-100 nm MOSFETs due to quantum effects: A 3-D density-gradient simulation study. IEEE Trans. Electron Devices **48**(4), 722–729 (2001)
22. Maes, R., Tuyls, P., Verbauwhede, I.: A soft decision helper data algorithm for SRAM PUFs. In: International Symposium on Information Theory, pp. 2101–2105 (2009)
23. Nangate 45 nm open cell library. http://www.nangate.com
24. Synopsys: HSPICE User Guide: Basic Simulation and Analysis (2016)
25. Petura, O., Mureddu, U., Bochard, N., Fischer, V., Bossuet, L.: A survey of AIS-20/31 compliant TRNG cores suitable for FPGA devices. In: International Conference on Field Programmable Logic and Applications (FPL), pp. 1–10 (2016)
26. Bernstein, D.J., et al.: Factoring RSA keys from certified smart cards: coppersmith in the wild. In: ASIACRYPT, pp. 341–360 (2013)