Challenges in Generating True Random Numbers Considering the Variety of Corners, Aging, and Intentional Attacks

Javad Bahrami*, Jean-Luc Danger†, Mohammad Ebrahimabadi*, Sylvain Guilley‡†, and Naghmeh Karimi*

*University of Maryland Baltimore County, United States
†LTCI, Télécom Paris, Institut Polytechnique de Paris, France
‡Secure-IC S.A.S., France

2023 International Conference on IC Design and Technology (ICICDT) | 979-8-3503-1931-6/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICICDT59917.2023.10332319

***Abstract*—True Random Number Generators (TRNGs) are sensitive Intellectual Property (IP) blocks involved in the creation of cryptographic keys, initialization vectors, nonces, etc. They must behave properly within a large environmental spectrum, including multiple corners, in case of aging-induced change of device characteristics over time, and also under intentional attacks aiming at lowering the TRNGs entropy.**

In this paper, we review normative and technical landscapes in this respect, and propose a pre-silicon verification methodology to assess the resilience of TRNGs. In particular, we qualify the unitary free running oscillator (FRO) entropy source analytically, and then extend the study to a full FRO-based IP module. Our results encompass analytical characterizations in terms of jitter measurements and certification-based characterizations in terms of tests.

***Index Terms*—TRNG, aging, attacks, free-running oscillators (FRO), jitter estimation, NIST randomness tests.**

I. Introduction

Digital chips are now entrusted to manage cryptographic keys. It is thus important in the first place to ensure that keys are generated securely. True Random Number Generators (TRNGs) are integrated devices that spawn keys. In fact, the role of TRNGs encompasses not only generating keys, but also initialization vectors, nonces, noise in Post-Quantum Cryptographic algorithms, and masks aiming at randomization countermeasures against side-channel analysis, amongst other security-related uses.

The field of TRNGs is rich, in that multiple hardware structures exist. Some are based on the initial state of memory upon power-up. Symmetrically, others are based on the decay time of DRAM. Others exploit races in an SR-latch structure, whilst eventually some TRNGs are based on the accumulated jitter in free-running ring oscillator (FRO) structures.

The diversity in TRNG types comes with pros and cons, in terms of PPA (power, performance, and area), entropy rate, resilience to aging & attacks, etc. One figure of merit that is often overlooked is to keep the TRNG properties over time. Indeed, degradation over time may compromise security in the long run. It is also an avenue for attackers to wear out the TRNG on purpose, so as to weaken it or even destroy it altogether.

Aging: Some standards document physical attacks threatening the TRNGs. In general, a TRNG must thus not only work correctly at birth but also be capable of enduring aging and/or attacks. The natural question that arises is thus: which TRNGs withstand such harsh conditions, which ones can be made resistant, and which ones collapse after some time? This paper provides inputs regarding TRNGs intrinsic resistance to aging and therefore can help designers opt for the most appropriate one, depending on their use case.

Certification and Normative Requirements: For instance, the Common Criteria (CC [5]) Protection Profile PP-0084 [6] models a forced leakage (`T.Leak-Forced`) caused by an active attacker. Also, PP-0117 [7] mentions that a compliant chip shall avert the threat of a deficiency of TRNG (`T.RND`).

Outline: The rest of the paper is structured as follows. A scholar background in device aging is given in Sec. II. The state of the art about the aging effect on TRNGs is surveyed in Sec. III. Then we address a missing point from the literature, namely the aging effect on a FRO-based TRNG, in Sec. IV. This section also unveils and leverages a novel method to simulate dynamic noise at HSpice level. We discuss results in Sec. V. Conclusions and perspectives are given in Sec. VI.

II. Background on Device Aging

Aging mechanisms result in performance degradation and eventual failure of digital circuits over time. Bias Temperature Instability (BTI) and Hot Carrier Injection (HCI) [1] are the two leading aging mechanisms affecting CMOS circuitries where both result in increasing switching voltage and path delays. NBTI (Negative BTI) [1] and PBTI (Positive BTI) affect PMOS and NMOS transistors respectively. HCI also affects NMOS devices.

BTI Aging: A PMOS (resp. NMOS) transistor goes under two phases of NBTI (resp. PBTI) depending on its operating condition [2]. The first phase, i.e., *stress*, occurs when the related transistor is “ON”. Here, charges are trapped at the

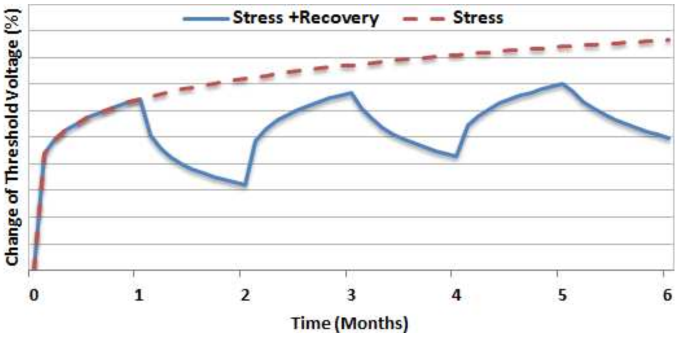


Figure 1. NBTI-induced V_{th} drift of a PMOS transistor that is always under the stress, and a transistor that is under the stress and recovery alternatively.

Si-SiO$_2$ interface and lead to an increase in the threshold voltage. The second phase, i.e., *recovery*, occurs when the transistor is off. In this phase, the charges trapped in the stress phase are partially removed, and thus the threshold voltage (V_{th}) drift that occurred during the stress phase partially recovers. The impact of BTI depends on the supply voltage, temperature, physical parameters of the transistor under stress, and stress time. Fig. 1 depicts the V_{th} drift of a PMOS transistor when it is continuously under stress for 6 months versus the case that it experiences stress and recovery phases every other month. In this figure, the values on the Y-axis are not shown intentionally to make the figure generic and technology independent.

HCI Aging: HCI happens in an NMOS when hot carriers are injected into the gate dielectric during transistor switching and remain there. HCI is a function of switching activity; degrading the circuit by shifting the threshold voltage and drain current of stressed transistors. The threshold voltage drift induced by HCI depends on the activity factor of the transistor under stress, its temperature, clock frequency, and usage duration [15].

III. Related work on the impact of aging on TRNGs

Mitigating aging impacts in TRNGs has received a lot of attention in recent years. For example, to prevent aging impacts, Muthukumar et al. [14] insert a number of transistors to the targeted TRNG to control the input of the embedded transistors when the TRNG is not used. In this research, the authors target a specific type of RO-based TRNG, the so-called tetrahedral, which comprises several overlapping fast and slow loops to increase metastability. Indeed when the TRNG is not active, the augmented circuitry places the related PMOS and NMOS transistors in their recovery phase to compensate for the aging-induced changes occurring during the TRNG usage. Here the TRNG is only ON when the cryptosystem calls for a key to run a cryptographic algorithm.

SRAM-based TRNGs also suffer from aging impacts resulting in the decline of entropy during the course of usage. Enforcing a pre-deployment increase of entropy through controlled aging [11] is not helpful in many cases [19] as with aging acceleration of some cells before deployment to increase the entropy, all the cells do not observe the same aging rate during the course of usage as the fresh cells have a faster aging rate while the ones that were exposed to accelerated stress initially experience a slower rate of aging thus such balancing of ‘0’ and ‘1’ values may deteriorate after some time of usage. Wang et al. [19] rely on the periodic compensation by repeatedly powering up the SRAM chip and then holding its power-up state in order to preserve the entropy of the power-up states of an SRAM array during the course of usage (aging).

In the paper [9], the authors propose a system called Fingerprint Extraction and Random Numbers in SRAM (FERNS) that harnesses static identity and randomness from existing volatile CMOS memory. The study focuses on NBTI impacts and demonstrates that a cell storing a particular value tends to favor the opposite value during subsequent power-up. They show that NBTI is not a significant concern for their proposed scheme if the device is operating under normal conditions. However, if it is used maliciously under atypical conditions, NBTI could be a threat to FERNS by providing a way to skew each cell toward a chosen power-up state.

Bahrami et al. target the SR-latch based TRNGs [1] that are composed of a number of SR-latches XORed to generate the final random number. They propose a stochastic model that can be used to decide about the number of latches required for a high entropy based on the knowledge of process mismatch and noise in the targeted chip and show that in such an SR-latch based TRNG the entropy improves over the course of aging if the mismatch to noise ratio is not too high. They also demonstrate that the mean of the process mismatch should be relatively small compared to the noise level to keep a minimum number of latches near a metastable state and in turn, provide a high level of entropy.

In [17], the authors develop a TRNG based on the remanence effects in DRAM relating to the condition where information remains in DRAM cells even after powering off. The proposed approach involves initially setting all cells to ‘1’, then turning off the memory for a specific delay period, and subsequently turning it back on. As DRAMs do not actually settle to all ‘0’ when powered off completely, they can be a good source of entropy to be used as TRNGs. The impact of aging on DRAM transistors decay has been studied in [4], but no conclusion on DRAM-based TRNGs has been derived.

The randomness of TRNGs may be also affected by fault injection attacks. In this regard, [3] demonstrates the behavior of TRNGs (mainly RO-based TRNGs) when aggressively targeted via ElectroMagnetic (EM) stress-induced faults. This study targets RO-based TRNGs and shows that the behavior of these TRNGs could be manipulated based on the strength and frequency of the faults injected via EM shots. Also in the context of fault injection attacks, [8] investigates if fault attacks targeting RO-based TRNGs can be self-induced or not. To do so the authors study the effects of harmonic injection attacks in

RO-based TRNGs where the frequency of the targeted TRNG is externally forced by a strong field; causing it to deviate from its intended oscillation frequency. The results demonstrate that the TRNG performs poorly when subjected to a strong coupling force. Table I summarizes the aforementioned state of the art in this area.

Table I
RELATED STATE OF THE ART ABOUT AGING EFFECTS ON TRNGS.

Proposed Method	**Aging Impact Analysis**	**Fault & EM Injection Analysis**
Muthukumar et al. [14] Tetrahedral RO-based TRNG	✓	×
Kiamehr et al. [11] SRAM-based TRNG	✓	×
Wang et al. [19] SRAM-based TRNG	✓	×
Holcomb et al. [9] SRAM-based (FERNS) TRNG	✓	×
Bahrami et al. [1] SR-Latch based TRNG	✓	×
Tehranipoor et al. [17] DRAM-based TRNG	×	×
Bayon et al. [3] RO-based TRNG	×	✓
Guilley et al. [8] RO-based TRNG	×	✓

* Red colors show the negative impact of the aging, green colors show the positive impact of the aging, and the blue color shows that the aging impact is different at different aging levels.

IV. AGING EFFECT ON RING OSCILLATOR BASED TRNGS

Impact of aging shall be carried out in all corners (at pre-silicon stage). In this section, we assume that one corner has been selected. Notice that it is intuitively clear that the performance of a TRNG will track in all corners, i.e., if the FRO-based TRNG improves over time for *one* corner, then such virtuous behavior is also expected from *any* corner.

A. Free-Running Ring Oscillator based TRNGs

As discussed earlier, one single FRO sampled by the system clock is easily manipulated externally by an attacker [3]. For this reason, we leverage the FRO-based TRNG rationale introduced in [12, Fig. 2, page 1193]. Therefore, in our experiments, one Free-Running Oscillator (FRO) is sampled by another FRO. This enables a differential mode, whereby external perturbation or adversarial influence is canceled out. One example is shown in Fig. 2, where the number of inverting components is odd so that the loop oscillates. In our simulations, the resynchronization flip-flop is not implemented; instead, the HSpice bench performs measurements on a regular basis to simulate the sampling by the system clock signal.

Obviously, in general, more than one such circuitry is required to get a fair amount of entropy. The output of those circuitries is then XORed with each other. The attained entropy can be extracted by the piling-up lemma [13].

Our setup adheres to the following details:

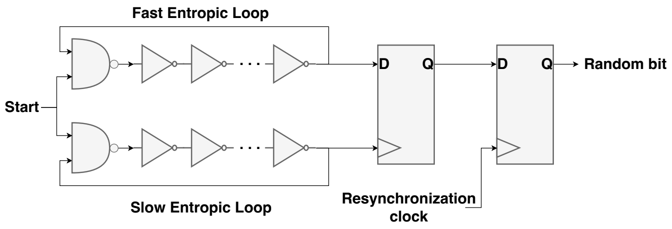


Figure 2. One single FRO-based TRNG structure.

- 19 inverting components (including 18 inverters and one NAND to start the entropic FRO to oscillate);
- 99 inverters in the sampling FRO, i.e., the one feeding the DFF clock signal. It must be slower than the entropic FRO, otherwise, we will capture stuttering sequences (e.g. $\underline{000}\overline{111}\underline{000}\overline{111}$, etc., assuming sampling is three times faster than the entropic FRO).

To investigate the effect of aging on the RO-Based TRNG, we performed the transistor level simulation in Synopsys HSpice using the 45 nm NANGATE technology. We utilized Monte-Carlo simulations with Gaussian distributions to account for process variation (PV) and replicate real-silicon behavior with the following specifications: transistor gate length L: $3\sigma = 10\%$, threshold voltage V_{TH}: $3\sigma = 30\%$, and gate-oxide thickness t_{OX}: $3\sigma = 3\%$. To model the aging, we employed HSpice built-in MOSRA (Metal-Oxide-Semiconductor Reliability Assessment) Level 3 model to extract NBTI, PBTI, and HCI aging effects (recall Section II). Aging is simulated for the usage of 7 years. The temperature of 85°C and voltage of 1.2 V are selected to simulate the circuit. Finally, the output of the TRNG is recorded every 5 ns on the HSpice measurement in the software (as mentioned earlier the resynchronization flip-flop is not implemented here).

B. Simulating Jitter in HSpice

For modeling the noise existing in real silicon in our HSpice simulations, we utilized three different methods: using the thermal noise of a resistor, deploying the thermal noise of transistors, and adding artificial noise to the power supply. We considered 10% voltage fluctuation as noise on the power supply of the circuit. As shown in Fig. 3(a), first we modeled the noise by adding a resistor to the power supply line of the circuit. Thermal noise may affect any electronic device and results from the random motion of charge carriers due to their thermal energy. For resistors, thermal noise spectral density is equal to $\overline{V_n^2}/\Delta f = 4KTR$, where K is the Boltzmann's constant, T is the temperature of the resistor in Kelvin, and R represents the resistor value. This noise is independent of the circuit frequency and can be tuned easily by changing the value of R. However, with high values of R, the voltage drop may go beyond the accepted value and thus affecting the performance and consequently, the entropy of the TRNG. For having 10% noise around $1.2V$ supply voltage, we slightly increased the voltage to compensate for the IR drop on the resistor.

The second method for modeling the noise in our setup is utilizing the thermal noise of the channel of MOS transistors shown in Fig. 3(b). The noise spectral density of an NMOS transistor is equal to $\overline{I_n^2}/\Delta f = 4KT\gamma g_m$ where γ is the thermal noise coefficient. This value is around $\frac{2}{3}$ for long-channel devices and around 2 for more advanced (short-channel) technologies. Moreover, g_m is the transistor's transconductance which depends on the bias and the transistor sizing. By sizing the buffer properly (driving strength of more than X1), the voltage drop gets compensated and the supply voltage gets noisy at the same time. Also, we have another source of noise which is called flicker noise–also called $1/f$ noise, which has inverse dependence on frequency as shown in Fig. 3(c). In our setup, considering the operating frequency, we can safely disregard this noise source as it gets dumped at frequencies higher than a couple of MHz (f_c). Here the main source of noise would be the thermal noise mentioned earlier.

Finally, for the third noise model, we generate a software-based noise and import this noise to the HSpice simulation. To do so here we augment the 1.2V nominal with a Gaussian noise between ±0.06V which is ±5% of power supply. Although we got similar results (output entropy) using these three methods, we only demonstrate the results of the third one, for the sake of space.

C. Unitary characterization setup

In order to investigate the effect of aging on the ring oscillator, we performed an HSpice simulation on a ring oscillator with 99 inverters over the course of 7 years with the aging step of 1 year. Figure 4 shows the distribution of the ring oscillator frequency while 10% noise (third method discussed above) is augmented to the voltage supply of the ring oscillator. As we explained, this noise on the voltage supply represents the jitters of the ring oscillator.

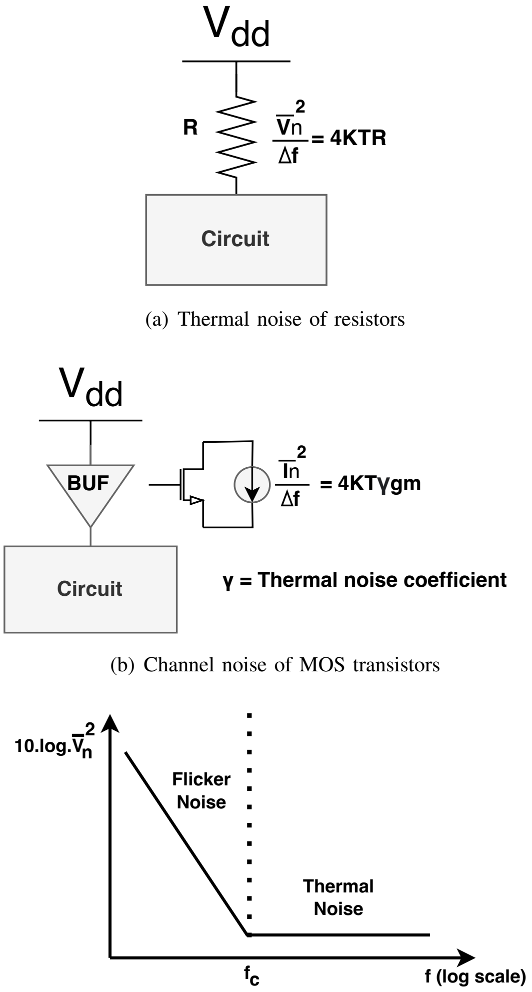
As depicted in Fig 4, the ring oscillator frequency is decreased from 1039 ps for the new device to 1211 ps for the 7-year-old device. Also, another observation that can be made from these results is the increase of the standard deviation of the ring oscillator's frequency (also known as the *jitter*) when the device is aged. The increase of the jitter's variance is a fundamental parameter to enhance the entropy of the TRNG as exploited in many TRNG architectures like in [18] which leverages the Phase Locked Loop (PLL block) of an FPGA. The takeaway point from this observation is that the entropy of the RO-based oscillators improves over the course of usage.

D. Source characterization

To show how aging affects the statistical properties of the RO-based TRNG, we ran the NIST FIPS SP 800-22 tests [16]. To do so we extracted a 1,100,000-bit stream from our fresh (non-aged) TRNG as well as our 7-year old TRNG. We divided this bit stream into 22 blocks each including 50,000 bits. Note that the majority of NIST tests do not have any block size requirement, e.g., randomness tests, yet a few NIST tests need a block size of one million bits (e.g., Universal test). As shown in Table II, aging could improve Frequency, Runs, Longest run, and Binary matrix tests. Although this table shows that some of the NIST tests fail, in real applications this is not happening as a number of RO-TRNGs (say dozens or even hundreds) are XORed in real silicon to attain a high entropy. Indeed, a single FRO structure is amenable to obtaining noise of *low entropy*, as shown in Fig. 5:

- a sampling rate larger than that of the entropic FRO causes *stuttering* (we, therefore, ensure by design that this situation does not happen), whereas
- a sampling rate smaller but related to that of the entropic FRO can cause *repetition sampling*, with low entropy.

To address this concern, we decided to XOR every 2 blocks (out of 10 blocks) where each block includes 22,000 bits and

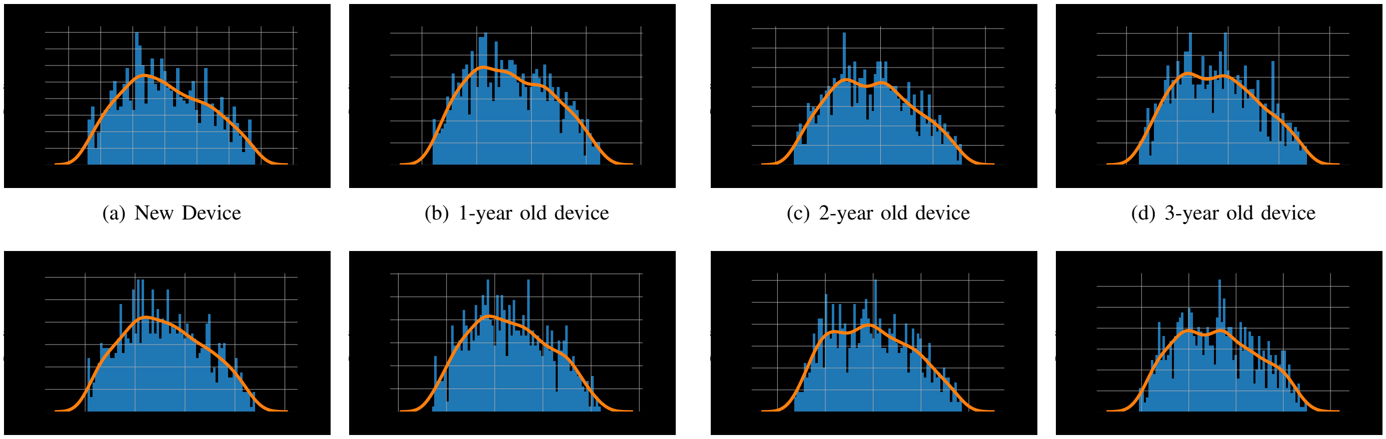

Vdd
R
$\frac{\overline{Vn}^2}{\Delta f}$ = 4KTR
Circuit
Vdd
BUF
$\frac{\overline{In}^2}{\Delta f}$ = 4KTγgm
Circuit
γ = Thermal noise coefficient
10.log.$\overline{V_n}^2$
Flicker Noise
Thermal Noise
f_c
f (log scale)

(a) Thermal noise of resistors

(b) Channel noise of MOS transistors

(c) Thermal vs. flicker noise

Figure 3. Noise modeling setup.



(a) New Device

(b) 1-year old device

(c) 2-year old device

(d) 3-year old device

(e) 4-year old device

(f) 5-year old device

(g) 6-year old device

(h) 7-year old device

Figure 4. Distribution of the time intervals between poisoning two bundles for different buffer & bundle sizes.

generates altogether 5 blocks of 22,000 bits for the NIST test.

Table II
NIST TEST RESULT RUNNING ON THE SINGLE FRO OUTPUT BOTH FOR FRESH AND AGED CIRCUITS.

Test	Age 0		7-year Aged	
	Pass/Total	P Value	Pass/Total	P Value
Monobit	22/22	0.594	20/22	0.452
Frequency	21/22	0.895	21/22	0.948
Runs	0/22	0	6/22	0.095
Longest Run	22/22	0.471	22/22	0.503
Binary Matrix	7/7	0.425	7/7	0.319
DFT	14/22	0.086	0/22	0
Non Overlapping	5/22	0.070	2/22	0.043
Overlapping	0/1	0	0/1	0
Universal	1/1	0.956	1/1	0.881
Linear Complexity	1/1	0.079	1/1	0.175
Serial	0/22	0.018	0/22	0.003
Approximate Entropy	0/22	0	0/22	0
Cumulative Sums	22/22	0.649	21/22	0.578
Random Excursion	1/1	0.304	1/1	0.320
Random Excursion Variant	1/1	0.57	0/1	0.362

Table III
NIST TEST RESULT RUNNING ON THE FULL-FLEDGED FRO-BASED TRNG OUTPUT BOTH FOR FRESH AND AGED CIRCUITS.

Test	Age 0		7-year Aged	
	Pass/Total	P Value	Pass/Total	P Value
Monobit	5/5	0.509	5/5	0.509
Frequency	5/5	0.406	5/5	0.392
Runs	5/5	0.572	5/5	0.572
Longest Run	5/5	0.492	5/5	0.282
Binary Matrix	1/1	0.051	1/1	0.296
DFT	5/5	0.438	5/5	0.335
Non Overlapping	5/5	0.537	5/5	0.507
Overlapping	*	*	*	*
Universal	*	*	*	*
Linear Complexity	*	*	*	*
Serial	5/5	0.589	5/5	0.673
Approximate Entropy	5/5	0.651	5/5	0.737
Cumulative Sums	5/5	0.481	5/5	0.634
Random Excursion	*	*	*	*
Random Excursion Variant	*	*	*	*

Table III shows that after XORing both fresh and aged devices can pass the NIST tests. Please note that for some of the NIST tests such as overlapping, as we do not have enough bit-stream we could not report the test results.

V. Discussion

The resistance of TRNGs in front of aging (and attacks) is an important engineering topic. However, we notice that the state of the art is poor in this respect. For the first time, we address the question of aging regarding FRO-based TRNG. This exploration is successful in terms of industrial deployments as aging does improve the entropy rate. Moreover, we underline that our method is the first to allow studying at the pre-silicon stage the effect of noise on aged devices. Those results would now deserve experimental validation in terms of real-world or accelerated aging tests, such as those precognized by the JEDEC association [10].

VI. Conclusion

In this paper, we have explored the impact of aging on TRNGs in general. We have deepened the study of free-running oscillators. In general, aging is nefarious to the amount of produced entropy. We studied the FRO-based TRNGs, in particular the architecture where the entropic FRO is sampled by another FRO. We show that FRO's produced entropy is not degraded as other TRNGs. This positions the FRO-based TRNG ideally for secure designs.

Acknowledgments

This work has partly benefited from the bilateral MESRI-BMBF project "APRIORI" from the ANR cybersecurity 2020 call (Project ANR 20-CYAL-0007), and in part by the

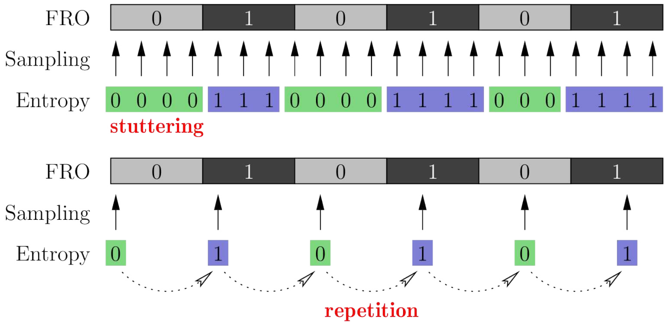


Figure 5. Defects inherent to a single entropy source, manifesting both when sampling is faster than the FRO (*top*) and when sampling is slower than the FRO (*bottom*).

National Science Foundation CAREER Award (NSF CNS-1943224). Besides, the authors acknowledge financial support of the French National Bank (BPI) under SECURYZR-V grant (Contract n° DOS0144216/00), a RISC-V centric platform integrating security co-processors.

REFERENCES

[1] Javad Bahrami, Mohammad Ebrahimabadi, Jean-Luc Danger, Sylvain Guilley, and Naghmeh Karimi. Special Session: Security Verification & Testing for SR-Latch TRNGs. In *2023 IEEE 41st VLSI Test Symposium (VTS)*, pages 1–10, 2023. San Diego, CA, USA.

[2] Javad Bahrami, Mohammad Ebrahimabadi, Jean-Luc Danger Danger, Sylvain Guilley, and Naghmeh Karimi. Leakage Power Analysis in Different S-Box Masking Protection Schemes. In *2022 Design, Automation & Test in Europe Conference & Exhibition, DATE 2022, Grenoble, France, March 14-23, 2022*. IEEE, 2022.

[3] Pierre Bayon, Lilian Bossuet, Alain Aubert, Viktor Fischer, François Poucheret, Bruno Robisson, and Philippe Maurine. Contactless electromagnetic active attack on ring oscillator based true random number generator. In *Proceedings of the Third international conference on Constructive Side-Channel Analysis and Secure Design*, COSADE'12, pages 151–166, Berlin, Heidelberg, 2012. Springer-Verlag.

[4] Md Kawser Bepary, Bashir Mohammad Sabquat Bahar Talukder, and Md Tauhidur Rahman. DRAM Retention Behavior with Accelerated Aging in Commercial Chips. *Applied Sciences*, 12(9), 2022.

[5] Common Criteria Consortium. Common Criteria (*aka* CC) for Information Technology Security Evaluation (ISO/IEC 15408), 2013. Website: http://www.commoncriteriaportal.org/.

[6] Eurosmart. Security IC Platform Protection Profile with Augmentation Packages (PP 0084), January 13 2014. BSI-CC-PP-0084-2014. Version 1.0. https://www.commoncriteriaportal.org/files/ppfiles/pp0084b_pdf.pdf.

[7] Eurosmart. Secure Sub-System in System-on-Chip (3S in SoC) Protection Profile (PP 0117), June 9 2021. https://www.eurosmart.com/secure-sub-system-in-system-on-chip-3s-in-soc-protection-profile/.

[8] Sylvain Guilley and Youssef El Housni. Random Numbers Generation: Tests and Attacks. In *2018 Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2018, Amsterdam, The Netherlands, September 13, 2018*, pages 49–54. IEEE Computer Society, 2018.

[9] Daniel E. Holcomb, Wayne P. Burleson, and Kevin Fu. Power-Up SRAM State as an Identifying Fingerprint and Source of True Random Numbers. *IEEE Trans. Computers*, 58(9):1198–1210, september 2009.

[10] JEDEC SOLID STATE TECHNOLOGY ASSOCIATION STANDARD. JESD22-A108G: Temperature, Bias, and Operating Life, November 2022.

[11] Saman Kiamehr, Mohammad Saber Golanbari, and Mehdi Baradaran Tahoori. Leveraging aging effect to improve SRAM-based true random number generators. In David Atienza and Giorgio Di Natale, editors, *Design, Automation & Test in Europe Conference & Exhibition, DATE 2017, Lausanne, Switzerland, March 27-31, 2017*, pages 882–885. IEEE, 2017.

[12] David Lubicz and Nathalie Bochard. Towards an oscillator based TRNG with a certified entropy rate. *IEEE Trans. Computers*, 64(4):1191–1200, 2015.

[13] Mitsuru Matsui. Linear Cryptanalysis Method for DES Cipher. In Tor Helleseth, editor, *Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings*, volume 765 of *Lecture Notes in Computer Science*, pages 386–397. Springer, 1993.

[14] Arunachalam Muthukumar, Narasimhan Sivasankari, and Kaniram Rampriya. Anti-aging true random number generator for secured database storage. In *2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS)*, pages 1–7, 2017.

[15] Fabian Oboril and Mehdi B. Tahoori. ExtraTime: Modeling and analysis of wearout due to transistor aging at microarchitecture-level. In *DSN*, pages 1–12, 2012.

[16] Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, Elaine Barker, Stefan Leigh, Mark Levenson, Mark Vangel, David Banks, Alan Heckert, James Dray, and San Vo. SP 800-22: A Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications, april 2010. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-22r1a.pdf.

[17] Fatemeh Tehranipoor, Wei Yan, and John A. Chandy. Robust hardware true random number generators using DRAM remanence effects. In *2016 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pages 79–84, 2016.

[18] M. Drutarovsky V. Fischer. True Random Number Generator Embedded in Reconfigurable Hardware. In *Proc. the 4th International Workshop on Cryptographic Hardware and Embedded Systems*, 2002.

[19] Wendong Wang, Ujjwal Guin, and Adit D. Singh. Aging-Resilient SRAM-based True Random Number Generator for Lightweight Devices. *J. Electron. Test.*, 36(3):301–311, 2020.