This is the peer reviewd version of the followng article:

Guidelines for the Design of Random Telegraph Noise-Based True Random Number Generators / Zanotti, T.; Ranjan, A.; O'Shea, S. J.; Raghavan, N.; Thamankar, R.; Pey, K. L.; Puglisi, F. M.. - In: IEEE TRANSACTIONS ON DEVICE AND MATERIALS RELIABILITY. - ISSN 1530-4388. - 24:2(2024), pp. 184-193. [10.1109/TDMR.2024.3394576]

Terms of use:

The terms and conditions for the reuse of this version of the manuscript are specified in the publishing policy. For all terms of use and more information see the publisher's website.

28/04/2026 13:49

(Article begins on next page)

Guidelines for the Design of Random Telegraph Noise-based True Random Number Generators

Tommaso Zanotti, *Member, IEEE,* Alok Ranjan, Sean J. O'Shea, Nagarajan Raghavan, *Member, IEEE*, Ramesh Thamankar, Kin Leong Pey, *Senior, IEEE*, Francesco Maria Puglisi, *Senior, IEEE*

***Abstract*— The development of a robust and secure hardware for the Internet of Things (IoT) and edge computing requires improvements in the existing low-power and low-cost hardware security primitives. Among the various available technologies, true random number generators (TRNGs) that leverage random telegraph noise (RTN) from nanoelectronics devices have emerged as effective solutions. However, the temporal instabilities in the RTN signal, such as the DC drift and temporary inhibition, are a few of the key reliability challenges for the TRNG circuits. In this study, we have utilized experimental RTN data collected from the commonly used gate dielectrics, including silicon dioxide (SiO_2), hafnium dioxide (HfO_2), and 2D crystalline hexagonal boron nitride (h-BN) to identify the crucial reliability challenges for RTN-based TRNG circuits. We have analyzed the impact of RTN instabilities and of circuit parameters on the output randomness and propose reliability aware design guidelines. Finally, we design and simulate an RTN-based TRNG circuit using a 130 nm CMOS technology and evaluate its reliability at the circuit level.**

***Index Terms*— Random Telegraph Noise (RTN), True Random Number Generator (TRNG), RTN instability, Circuit reliability, Gate dielectrics.**

I. INTRODUCTION

WITH the diffusion of edge computing and Internet of Things (IoT) devices, there is a growing demand for the development of a low-power and a low-cost hardware security primitives [1], [2], [3] that can be fabricated directly on the chip to support the foundation of a hardware Root-of-Trust [4]. Among these hardware security primitives, True Random Number Generators (TRNGs) play a pivotal role in various cryptography-related tasks [5]. For instance, TRNG circuits have been employed to periodically update encryption keys on a system to protect data exchanged either intra or inter chips. As the CMOS technology approaches its scaling limits, researchers are exploring the stochastic properties of materials and nanoelectronics devices beyond CMOS for the hardware security applications [1], [2], [6], [7]. Nanoelectronics devices provide diverse sources of entropy, with Random Telegraph Noise (RTN) emerging as a promising solution for designing low-power TRNG circuits [8], [9], [10], [11]. RTN is a phenomenon commonly observed in scaled nanoelectronics devices which employ thin dielectric films e.g., transistors and resistive switching devices [12]. RTN is associated with a stochastic capture and emission of charge by the atomic defects within the dielectric material, resulting in the generation of a high-entropy signal. For example, RTN in most common gate dielectrics (i.e., SiO_2 and HfO_2) is generally associated with the activity of oxygen vacancy defects. It has been observed experimentally that the properties of RTN signals, such as trap time constants and the number of levels, often exhibit instability over time. Both we and other have shown using calculations that these temporal changes in the RTN in HfO_2 are associated with the electrostatic interactions among oxygen vacancy defects and/or the diffusion of the defects within the dielectric [13], [14], [15]. These temporal instabilities in the RTN signal could affect the reliability of RTN-based TRNG circuits and this is yet to be understood. In this work, we extend our conference paper [16] where experimentally measured RTN data from three distinct gate dielectrics were employed in circuit simulation to i) estimate their suitability for TRNG applications, ii) identify potential reliability issues due to the RTN temporal instabilities in the existing RTN-based TRNG circuits, and iii) propose the integration of multiple noise sources as a solution to improve RTN-based TRNG circuits robustness. Here, we have extended the previous analysis linking RTN characteristics to circuit design parameters and have developed specific reliability-aware design guidelines. Finally, we have discussed the critical reliability issues arising in integrated circuit implementations and qualitatively analyzed them on a TRNG designed using the SGS13 130 nm technology from IHP [17].

II. RTN MEASUREMENT AND ANALYSIS

A. Test structures and measurement setup

RTN was measured from three different test structures that employ different dielectric materials, i.e., HfO_2, h-BN, and SiO_2. The test structures are sketched in Fig. 1, and comprise of

T. Zanotti and F. M. Puglisi acknowledge financial support from PNRR MUR project ECS_00000033_ECOSISTER. T. Zanotti acknowledges the financial support of the FAR Dipartimentale 2023 project "RESISTRONG". *(Corresponding author: Tommaso Zanotti).*

T. Zanotti, and F. M. Puglisi are with the Dipartimento di Ingegneria "Enzo Ferrari," Università degli studi di Modena e Reggio Emilia, 41125 Modena, Italy.

A. Ranjan is with the Department of Physics, Chalmers University of Technology, Gothenburg, 412 96, Sweden.

S. J. O'Shea is with the Institute of Materials Research and Engineering, Agency for Science Technology and Research, 2 Fusionopolis Way, Singapore.

N. Raghavan, and Kin Leong Pey are with the Engineering Product Development, Singapore University of Technology and Design, 8 Somapah Road, Singapore.

R. Thamankar is with the Centre for Functional Materials, Vellore Institute of Technology, Vellore, India.

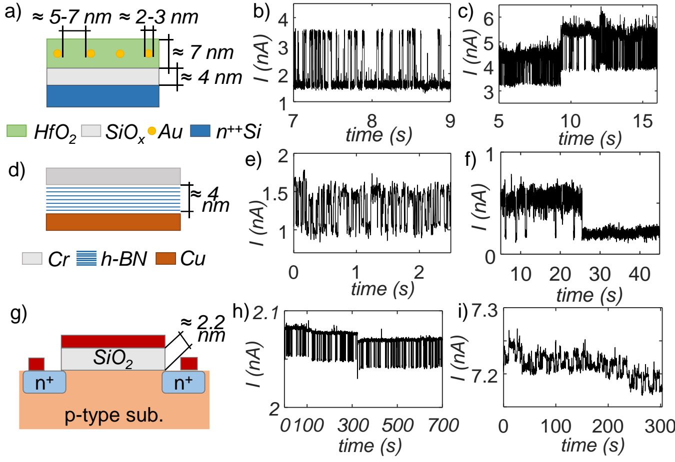

Fig. 1. a), d), g) Sketch of the three test structures measured in this study. Example of measured 2-level RTN in b), e), and h). Examples of measured complex RTN in c), f), and i).

a) an HfO_2 dielectric embedded with Au nanocrystals that were introduced to enhance the defect generation and also to create preferential path for the dielectric breakdown by modulating the electric field in the dielectric in the vicinity of the Au nanocrystal [18], *b)* a commercially available multi-layer h-BN (purchased from Graphene Supermarket®) grown on a polycrystalline copper substrate by chemical vapor deposition [19], and *c)* thermally grown 2.2 nm SiO_2 in a NMOS transistor test structure. The RTN in both HfO_2 and h-BN were measured using a conductive atomic force microscope (CAFM) operating in ultra-high vacuum. The CAFM was integrated with a Keithley 4200 semiconductor parameter analyzer and a current amplifier (FEMTO DLPCA-200) for an efficient collection of RTN data. The SiO_2-based transistor test structure was measured using a probe station. h-BN samples were measured both pre- and post- soft breakdown to investigate the variations in the RTN characteristics due to the soft breakdown.

B. RTN signal analysis

For the HfO_2, h-BN, and SiO_2 test structures a total of 319 s, 680 s, and 2910 s RTN data, were collected and analyzed, respectively. By visual inspection, 2-level RTN, i.e., the desired outcome, was measured from all test structures, see Fig. 1b, e, and h. However, also complex RTN showing different instabilities was measured from all test structures, see Fig. 1c, f, and i. Among the different types of RTN instabilities [20], DC level drift, multi-level RTN, temporary RTN [13], and mutant RTN [13] were observed from all dielectrics. These non-ideal RTN signals were analyzed as shown in Figs. 2-3 and characterized as follows. First for each of the signals a time-lag plot was realized to estimate the number of stable states in the RTN signals [21]. Then, the number of stable states is used as an input of Factorial Hidden Markov Model (FHMM) which enables to extract the statistical properties of the RTN signal, namely the dwell times and amplitude [22], [23]. To model RTN signals presenting instabilities the signal was split into segments with homogeneous properties, see Fig. 3a. The traps dwell times and amplitudes were taken into account for determination of an appropriate sampling frequency to be used

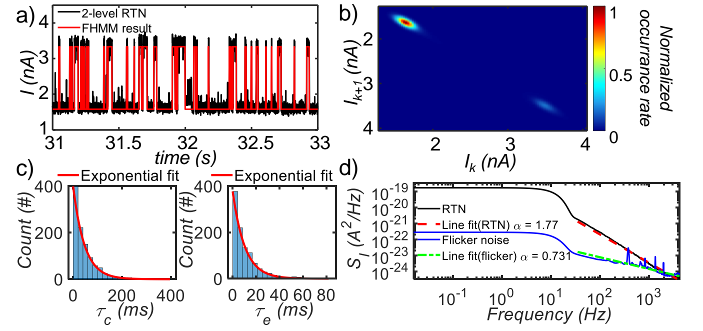

Fig. 2. a) Fitting of 2-level RTN from the HfO_2 test structure using FHMM. b) Time-lag plot of a), confirming the 2-level nature of the RTN. c) Capture and emission times distributions estimated with FHMM. d) PSD of the FHMM-extracted RTN (black line), and remaining flicker noise component (blue line), confirmed by PSD slopes (dashed lines). PSD estimated using Welch's method with a Hamming window of 512 samples and 50% overlap.

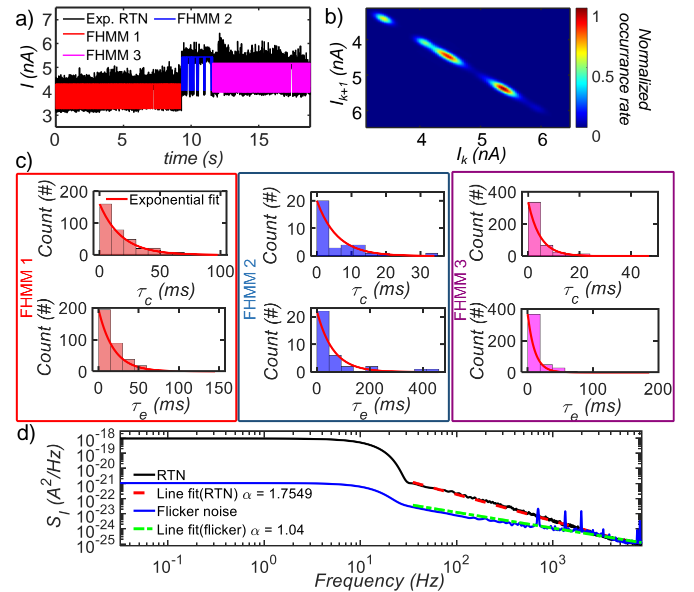

Fig. 3. a) Fitted with FHMMs of an RTN signal from the HfO_2 sample presenting several instabilities. Signal segmented and fitted separately. b) Time-lag plot of a), showing RTN level shifts along the diagonal. c) Capture and emission times distributions estimated with FHMMs. Notable changes in segment 2 (FHMM 2). d) PSD of the FHMM-extracted RTN (black line), and remaining flicker noise component (blue line), confirmed by PSD slopes (dashed lines). PSD estimated using Welch's method with a Hamming window of 512 samples and 50% overlap.

in the RTN-based TRNG circuits. The choice of sampling frequency is an important consideration so that the output bitstream achieves high randomness [24], [25], [26]. The estimated τ_0 (i.e., $\tau_0 = (\overline{\tau_c}^{-1}+\overline{\tau_e}^{-1})^{-1}$, where $\overline{\tau_c}$ and $\overline{\tau_e}$ are the average capture and emission time, respectively) and amplitude (i.e., ΔI) are reported in Table I for each of the analyzed signals. Also, the maximum frequency that can be adopted to sample a new random bit is reported in Table I. While the HfO_2, and h-BN

TABLE I
EXTRACTED TRAPS TIME CONSTANTS AND OPTIMAL RTN-TRNG SAMPLING FREQUENCY

Dielectric material	RTN characteristics	ΔI (nA)	τ_0 (ms)	Optimal* RTN-TRNG f_s (Hz)
HfO_2	2-level RTN	1.95	85	< 4
	RTN w Several instabilities	1.03 1.39 1.30	5.2 5.3 3.3	
	Mutant RTN	0.57 1.73	5.6 106	
h-BN	2-level RTN	0.40	14.5	< 5
	Mutant RTN	0.20 0.36 0.77	33.4 64.7 277	
	Temporary RTN	0.28	76	
SiO_2	2-level RTN	0.023	951	< 0.4
	RTN w DC-level drift	0.022 0.013 0.030	815 1040 1120	
	Temporary RTN	0.016	865	

*Considering the design constraints for reducing the autocorrelation of the output bitstream discussed in [24]-[26].

tests structures achieve a comparable maximum sampling frequency, the SiO_2 one achieves an order of magnitude lower maximum sampling frequency. Thus, this preliminary analysis suggests that SiO_2 test structure allows the implementation of RTN-based TRNGs with lower output throughput. Finally, to analyze the noise frequency content the power spectral density (PSD) of the different signal components was estimated using the Welch's method [27]. As shown in Figs. 2d, and 3d, the PSD was computed both on the FHMM outputs used to replicate each of the RTN signals and on the difference between original signals and the corresponding FHMM-extracted RTN. As expected, the FHMMs and the remaining noise showed a $1/f^2$, and $1/f$ spectrum, respectively, indicating that RTN signals are superposed to a background flicker noise, likely emerging from slower traps and additional intrinsic noise mechanisms [28]. In the following sections, the reliability of RTN-based TRNG circuits in the presence of RTN temporal instabilities is analyzed by adopting the experimental RTN signals and the results obtained from the above analysis.

III. RTN-BASED TRNGS: PRINCIPLES OF OPERATION

RTN-based TRNG circuits leverage on the stochastic nature of the capture and emission of charge from the atomic defects in a dielectric to generate a random bitstream. Specifically, the circuits use the abrupt transitions in the input RTN current/voltage signals to generate a random bitstream. Thus, typically RTN-based TRNGs require the functional building blocks shown in Fig. 4a [9], that are responsible for signal conditioning, detecting the defects capture and emission events, and generating the output random bitstream. The input stage is a Transimpedance Amplifier (TIA) which amplifies the small device current (i.e., few nA) and sets a virtual ground at the

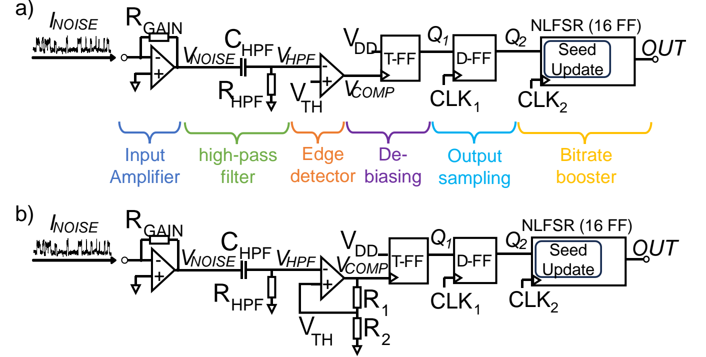

Fig. 4. RTN-based TRNG circuit implementations: a) fixed threshold comparator, b) comparator with hysteresis. Functional description for each subcircuit is available in a).

TRNG input to guarantee that a constant voltage bias is applied to the entropy sourcing device. However, the TIA amplifies both the DC component and the overlapped AC noise, thus making a filtering stage mandatory. Thanks to the abrupt characteristic of RTN, a High-Pass Filter (HPF) can be used to block the amplified DC component from the signal. A comparator is then used to detect capture or emission events. As shown in Fig. 4a-b, the comparator can be designed either with a fixed threshold or with a hysteresis. As shown in Fig. 5, the two circuits output different waveforms, but from the TRNG functioning standpoint the output result is identical. Nevertheless, the choice of using a fixed threshold or one with a hysteresis can have potential implications on the reliability of the TRNG when RTN signal instabilities appear, and thus both implementations are considered in this work. The output of the comparator is fed to the input of a Toggle Flip-Flop (T-FF), which debiases the sequence by toggling its output only upon detection of a new capture or emission event [25]. The absence of T-FF could result in an imbalanced distribution of zeros and ones in the output bitstream due to uneven average defects' capture and emission times (i.e., τ_c and τ_e), compromising randomness. The T-FF output is then sampled by a sample and hold (S&H) circuit, with a sampling frequency, as shown in Table I, set sufficiently lower than the inverse sum of the average defects' capture and emission times to prevent biasing the output bitstream [25]. As discussed in the previous section, depending on the material, device structure and measurement set-up, RTN may exhibit very slow average defects' capture and emission times, leading to low throughputs of the TRNG. Thus, a common solution employed to enhance the throughput is to use the output of the TRNG to periodically update the seed of a Pseudo Random Number Generator (PRNG) [9], [29], [30], such as a Nonlinear Feedback Shift Register (NLFSR) in this study (see Fig. 4). This approach capitalizes on the PRNG's, low area occupation, low-power consumption and higher throughput while maintaining output randomness through a reseeding strategy. In addition, the use of a NLFSR introduces a post-fabrication tunable circuit parameter (i.e., CLK_2/CLK_1) which allows to compensate for variations in defects time constants among different devices. In terms of the reliability of RTN-based TRNG circuits, effects related to both the entropy source device and the circuit can pose reliability challenges.

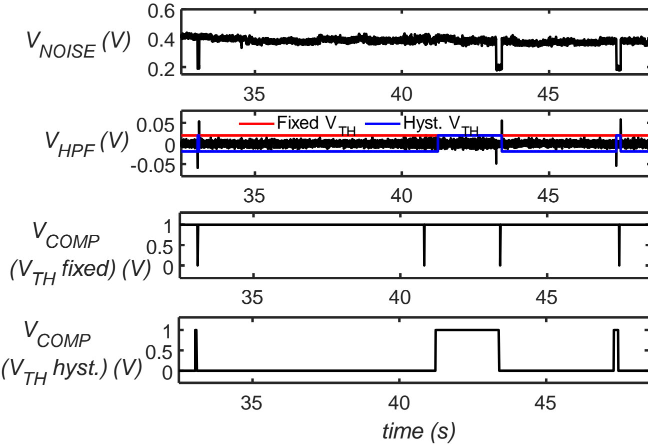

Fig. 5. Simulation results from various circuit nodes. Circuit tuned to harness only the $1/f^2$ component. Comparator output shown with fixed threshold (red line) or hysteresis (Blue line).

The subsequent sections delve into the reliability issues of RTN-based TRNG circuits, focusing initially on the effects of the entropy source device alone in Section IV, where a TRNG implemented with ideal components is simulated when input only stable 2-level RTN (i.e., the ideal condition) or 2-level RTN signals concatenated with non-ideal RTN signals. Subsequently, in Section VI we explore the combined effects of both device and circuit-related issues.

IV. Analysis of the Impact of RTN Signal Instabilities on the Reliability of RTN-Based TRNG Circuits

Various devices and material systems can result in RTN signals exhibiting diverse characteristics and levels of complexity [31]. Consequently, it becomes imperative to initially assess the suitability of these devices as entropy sources for TRNG applications. To isolate the impact of experimental factors (e.g., device structure and measurement set-up) on TRNG performance and reliability, the ideal RTN-based TRNG circuits shown in Fig. 4, was simulated using Cadence Virtuoso®. In the simulations, behavioral models for the operational amplifier (OPA) and digital circuit elements were adopted. Despite employing ideal models for various circuit components, the circuit's performance in extracting capture and emission events from the RTN signal is nonetheless influenced by different design parameters. Notably, the TIA, the HPF cutoff frequency, and the comparator threshold voltage (V_{TH}) collectively dictate the noise selectivity of the TRNG circuit. Following the conventional design approach of RTN-based TRNGs [24], [25], the circuit parameters were tuned so that only the noise transitions generated by a single defect (specifically, the $1/f^2$ component) were harnessed by the circuit. A demonstration of the circuit operation is shown in Fig. 5. To estimate the performance as entropy source of the test structures, the NIST randomness tests [32] were performed on the bitstream out of the circuit, which is utilized to reseed the NLFSR. While an output bitstream was computed for each test structure at the circuit node Q_2, the complete set of NIST tests could only be conducted on HfO_2 and h-BN after soft

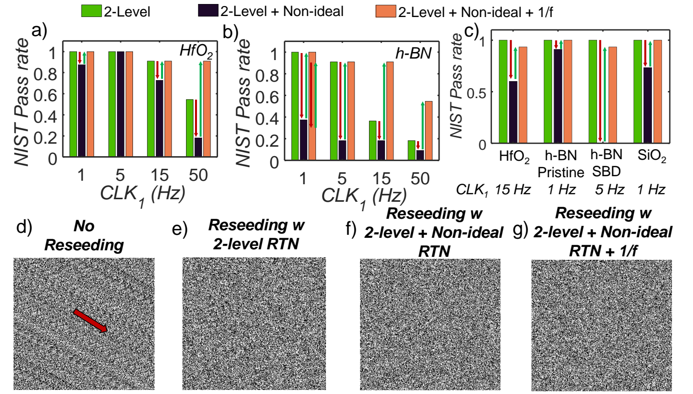

Fig. 6. a) and b) NIST randomness test pass rates for Q_2 node in Fig. 4a, with the circuit tuned for $1/f^2$ or both the $1/f^2$ and $1/f$ noise components, using ideal 2-level RTN signals alone or concatenated with non-ideal RTN signals. Improved randomness observed with $1/f$ noise component during non-ideal RTN. Results are shown for various sampling frequencies. c) NIST randomness test pass rates for the output OUT of the circuit in Fig. 4a. Similar tuning and inputs were used as in a) and b), with the $1/f$ noise component improving randomness during non-ideal RTN occurrance. CLK_1 frequencies indicated. d)–g) Confusion matrices generated from the 16-bit NLFSR output in Fig. 4a. Without reseeding d), clear pattern highlighted (red arrow). Periodic NLFSR reseeding e–g) yields apparently random confusion matrices. Simulations used HfO_2 test sample RTN data, CLK1 set to 15 Hz, representing a borderline case where the TRNG circuit is less robust to non-ideal RTN effects as shown in a). NIST tests passed with p-value > 0.01.

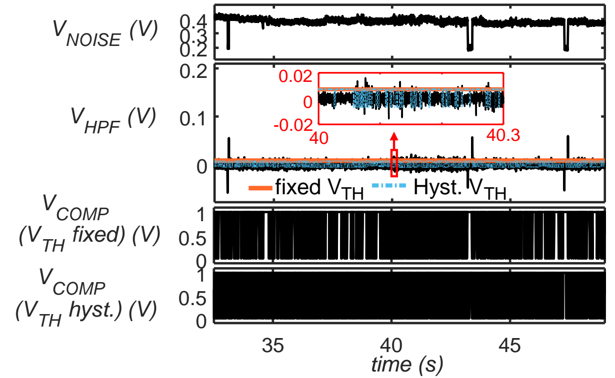

Fig. 7. Simulation results at various circuit nodes with circuit parameters tuned for harnessing both $1/f^2$ and $1/f$ noise components. Comparator output shown with fixed threshold (red line) and with hysteresis (dashed blue line).

breakdown (h-BN SBD) samples. The execution of the full test suite necessitates bitstreams of at least 10^6 bits, or a minimum of 387840 bits to perform 11 out of 15 tests (i.e., longest-run-of-ones in a block, linear complexity, random excursion and random excursion variant tests require input sequencies of longer than 10^6 bits [32]). However, due to the limited duration of experimentally collected RTN data and the slow defects' capture and emission times observed in SiO_2 and pristine h-BN-based samples, only shorter bitstreams could be generated. Figure 6a-b illustrates that under the condition where the circuit

is subjected to 2-level RTN signals and exploits sufficiently low sampling frequencies (CLK_1 in Fig. 4), both test structures yield a highly random output bitstream, successfully passing all NIST tests. This implies that in ideal conditions, RTN from h-BN and HfO_2 structures serves as a high-quality source of entropy. However, the introduction of non-ideal RTN signals which has temporal variations results in a rapid decrease in randomness (with the NIST approximate entropy, runs and the discrete Fourier transform (DFT) tests being the first to fail). This is particularly critical when the sampling frequency increases (refer to Fig. 6a-b), underscoring a significant reliability concern. Consequently, effective strategies must be adopted to either mitigate these adverse effects or enhance the reliability of RTN-based TRNGs in the presence of temporal instabilities in the RTN signal.

V. Increasing the robustness of RTN-based TRNGs to RTN instabilities

A. Harnessing both $1/f^2$ and $1/f$ noise components

We have investigated potential solutions for improving the TRNG circuit's resilience to non-ideal RTN signals by adjusting circuit parameters. Specifically, the HPF cut-off frequency and the comparator threshold voltage were altered to utilize both the $1/f^2$ and $1/f$ noise components as entropy sources. As shown in Fig. 7, this adjustment led to more frequent random transitions at the comparator output (V_{COMP}) for both the cases when a comparator with and without hysteresis was used. The increased activity at the output of the comparator ensures high randomness in the presence of non-ideal RTN signals. Even in scenarios where the 2-level RTN relative power diminishes (e.g., temporary RTN signals in Fig. 1f), appropriately tuned TRNG parameters enable the circuit to generate a random output. Consequently, optimal randomness is restored by harnessing the $1/f$ noise component, as illustrated in Fig. 6c. Although, designing TRNG circuit to exploit only the $1/f$ noise may seem sufficient to achieve high randomness, as flicker noise can evolve over time, neglecting RTN and signal instabilities can lead to unreliable TRNG designs appropriately considered in the design phase. Thus, RTN must be considered for high reliability and improved randomness.

B. Verification on high throughput random bit generation

The effectiveness of this compensation strategy was then evaluated on the NLFSR output (OUT in Fig. 4), which enhances TRNG throughput. To assess this strategy's impact, the circuit was simulated for each test structure using a sampling frequency (CLK_1) that yielded high TRNG randomness with 2-level RTN but started degrading with complex RTN. A 16-bits NLFSR was employed to simulate bitstreams consisting of multiple NLFSR periods. As shown in Fig. 6d, the NLFSR exhibits periodicity, and discernible patterns emerge in the confusion matrix without reseeding. Reseeding the NLFSR with various components of input RTN signals consistently produces seemingly random confusion matrices, as depicted in Fig. 6d-g. NIST randomness test results indicate that reseeding exacerbates randomness degradation

TABLE II
TRNG Performance comparison by test structure

Test structure	Stable 2-level RTN in TRNG input	Randomness loss*	Randomness Loss after Recovery**	Throughput (@ node *OUT*) w/ 16-bits NLFSR	Throughput (@ node *OUT*) w/ 24-bits NLFSR
HfO_2	≈ 61%	40%	6.7%	4468 bit/s	1.14 Mbit/s
h-BN Pristine	≈ 81%	9.1%	0%	936 bit/s	240 kbit/s
h-BN after SBD	≈ 11%	100%	6.7%	847 bit/s	217 kbit/s
SiO_2	≈ 81%	26.7%	0%	304 bit/s	77.8 kbit/s

*Reduction in NIST test pass rate due to nonideal RTN, expressed as a percentage. **NIST pass rate reduction when exploiting also the *1/f* noise component. NIST tests passed with p-value > 0.01.

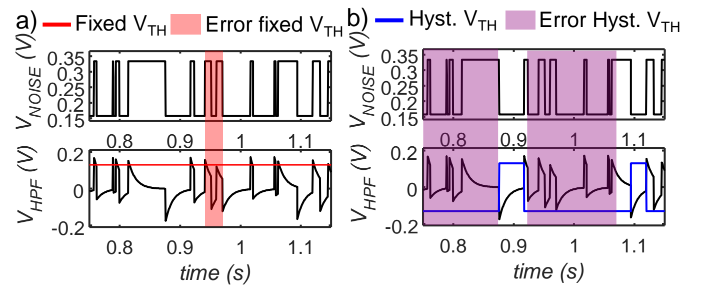

Fig. 8. RTN transition detection error caused by a bad design of the HPF and comparator threshold, when a) the comparator has a fixed threshold, and b) the comparator employs a hysteresis.

when only harnessing the $1/f^2$ noise (with the approximate entropy, DFT, longest-run-of-ones in a block, and the serial tests commonly failing). The result show that combining both the $1/f^2$ and $1/f$ noise components achieves high randomness for bitstreams longer than the NLFSR period (i.e., $2^{16} - 1 = 65535$), even with non-ideal RTN signals, as shown in Fig. 6c and Table II. Furthermore, in Table II we compare the performance of the three test structures for TRNG applications. In terms of randomness, the h-BN sample after SBD, which produces more unstable RTN compared to the other test structures, is most affected by non-ideal RTN signals, resulting in a predictable bitstream, followed by the HfO_2-based test structure. However, the lost randomness is recovered when the $1/f$ noise component is used. Regarding TRNG throughput, the HfO_2 sample achieves the highest throughput among the three test structures, with the SiO_2 sample achieving the lowest. Nevertheless, the periodic reseeding must be performed a sufficient number of times (i.e., > 200 times for the three test structures in this work) during each NLFSR period to ensure effectiveness. Thus, the maximum achievable throughput is adversely impacted by lower sampling frequencies (CLK_1). By increasing the number of registers in the NLFSR the TRNG throughput could be improved from a few kbit/s to Mbit/s, depending on the target applications in IoT and edge computing [33], [34]. It also implies that if the SiO_2 device has to achieve a throughput

comparable to other material systems, this would require a larger chip area to fabricate an NLFSR with more registers.

VI. Reliability-aware design strategies

From the previous analysis it is clear that for achieving high randomness, RTN-based TRNG circuits must be designed to work in a specific functioning operating range to ensure that the circuit can generate highly random output bitstreams despite RTN temporal instabilities. Thus, to develop reliability-aware design strategies, it is important to identify the main circuit design parameters that could influence the TRNG operation and reliability. In this section, we exploit the result of the RTN signals analysis in Section II.B, and of circuit simulations performed on the circuits in Fig. 4, to study the impact of different circuit parameters on the TRNG circuit operation and to determine appropriate reliability-aware design guidelines.

A. Impact of high-pass filter cut-off frequency and comparator threshold

The detection of RTN signal transitions is strongly influenced by the input amplifier gain, the HPF cut-off frequency, and the comparator threshold. Considering that the input amplification stage sufficiently amplifies the noise signal (i.e., $A_v = 10^8$), we analyze the combined effect of the HPF cut-off frequency and of the voltage threshold. In general, higher HPF cut-off frequencies enable to remove the DC component more effectively from the input RTN signal, and to achieve sharp transitions at the output of the filter in correspondence of RTN or 1/f noise transitions. However, increasing the HPF cut-off frequency results in spikes with lower amplitudes at the input of the comparator, thus reducing the tolerance to gain and voltage threshold variations. Conversely, reducing the HPF cut-off frequency, increases the amplitude at the input of the comparator, however, more of the low frequency component of the noise signal is kept, resulting in less sharp transitions at the output of the HPF, potentially leading to errors in the discrimination of consecutive charge capture/emission events. Thus, both the filter frequency and the comparator threshold influence the minimum temporal distance between consecutive capture or emission events that can be resolved by the circuit, i.e., the time resolution of the circuit. An example of errors related to the combined effect of HPF and V_{TH} is shown in Fig. 8. In general, when considering the comparator with hysteresis, this effect is more detrimental with respect to the case with a fixed threshold. This suggests that the use of a fixed threshold is a better choice for a reliability-aware design.

To estimate the circuit's minimum time resolution based on the HPF cut-off frequency and the comparator threshold, we devised a strategy employing the PSD and the FHMM reconstructed signal from Section II.B. Considering the TIA and HPF frequency responses, see Fig. 9a, we determined the amplitude of the spikes at the output of the HPF due to RTN transition for different cut-off frequency values. By analyzing the step response of the system, see Fig. 9b, the spike amplitude and the time constant of the system can be retrieved. This enables us to estimate the minimum time resolution of the

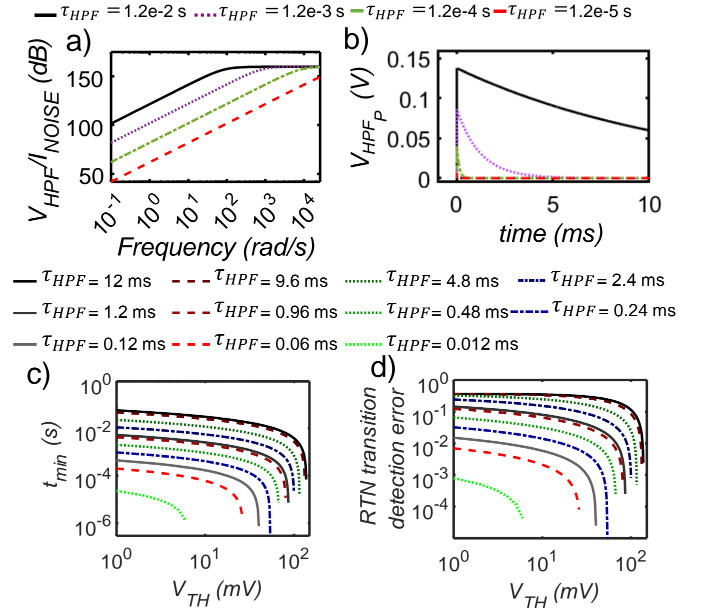

Fig. 9. a) TIA stage and HPF filter frequency response with varying filter time constant (τ_{HPF}). b) Step response for changing τ_{HPF}, considering RTN signal frequency content. c) Estimated minimum edge detection circuit time resolution for changing τ_{HPF} time constant and comparator voltage threshold (V_{TH}). d) Probability of RTN transition error detection with changing τ_{HPF}, and V_{TH}.

circuit and consequently the probability of missing one of two adjacent RTN transitions. For example, consider the case depicted in Fig. 8a inside the red rectangle, when the first capture event happens at the output of the HPF there is a spike which is proportional to the derivative of the signal. The amplitude of the spike and the filter time constant determine the time t_{min} for which the signal remains above the comparator threshold. Such t_{min} can be easily estimated using (1), where V_{HPF_p} is the peak amplitude of the spikes at the output of the HPF.

$$t_{min} = -\tau_{HPF} \ln\left(1 - \frac{V_{TH}}{V_{HPF_p}}\right) \quad (1)$$

After the charge emission, the subsequent capture event will result in a spike above V_{TH} only if (2) is verified.

$$\tau_e < \tau_c - t_{min} \quad (2)$$

Since both τ_e and τ_c follow exponential distributions, the probability that (2) is not satisfied and that the circuit misses the detection of an RTN transition is given by (3), where λ_c and λ_e are the inverse mean of the capture and emission times exponential distributions, respectively.

$$\mathbb{P}(\tau_c - \tau_e \geq t_{min}) = 1 - \mathbb{P}(\tau_c - \tau_e \leq t_{min}) = 1 - \frac{2\lambda_c}{\lambda_c + \lambda_e}\left(1 - e^{-\lambda_e t_{min}}\right) \quad (3)$$

This analysis was performed on the available RTN signals, and the results are shown in Fig. 9c-d for the HfO_2 sample. As expected, lower HPF cut-off frequencies result in better time resolution and fewer RTN transition detection errors, see Fig. 9c-d. However, the useful V_{TH} range shrinks due to reduced spikes amplitude, leading to a lower tolerance to variations.

It is also interesting to note that for each different HPF cut-

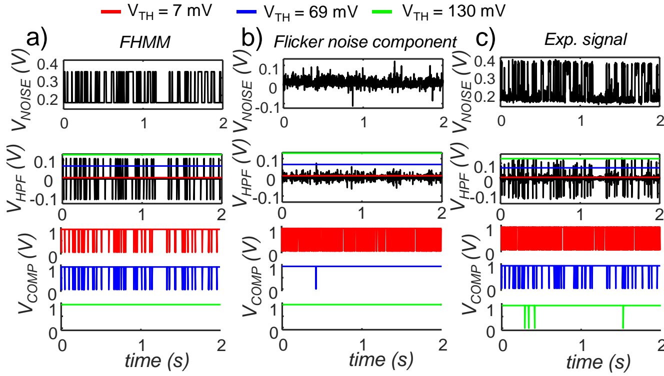

Fig. 10. Results of circuit operating regime analysis showing varying comparator voltage threshold effects on different signal components: FHMM reconstruction a), flicker noise b), and full signal c). For low V_{TH} values both $1/f^2$ and $1/f$ noise are exploited (red lines). Exceeding flicker noise amplitude isolates $1/f^2$ noise (blue lines). Higher thresholds may lead to circuit malfunction (green line).

off frequency the best time resolution and detection error rate are achieved when the voltage threshold is close to the step response amplitude. This condition, however, would set the circuit in an unstable operating condition in which small V_{TH} variations could potentially compromise the edge detection. We also wish to highlight that V_{TH} cannot be too high otherwise the *1/f* noise component would not be exploited by the circuit. Thus, to reduce the probability of missed detections, instead of increasing the comparator $V_{TH,}$ a more reliable approach would be to increase the HPF cut-off frequency. This is however constrained by a tradeoff between the HPF cut-off frequency and the tolerance to gain and V_{TH} variations.

B. Analysis and definition of circuit operating regimes

As mentioned above, when the HPF cut-off frequency and the input gain are determined, changing the voltage threshold can lead to different circuit operating regimes. As shown in Fig. 10, these can be divided in the three different operating regimes depending on the value of the voltage threshold. When using low $V_{TH,}$ both the $1/f^2$ and $1/f$ noise components contribute to the output entropy. This can be observed as an increased activity at the output of the comparator. By increasing V_{TH} the circuits becomes more selective and only the $1/f^2$ component is effectively harvested up until the voltage threshold becomes too high that the circuit is unable to detect any event. Thus, the circuit operates in a specific operating regime for a certain V_{TH} range, meaning that specific margins exist, and depend on the amplitude spectrum of the different noise components.

C. Tolerance to DC level drift

As also shown in Fig. 1c, the DC component of the RTN signal can drift over time. This phenomenon has detrimental effects on the reliability of RTN-based TRNG circuits. Generally, during the design phase the designer is prone to maximize the gain of the input gain stage, so that the amplitude of the spikes at the output of the HPF are maximized resulting in better t_{min} and increased tolerance to variations. However, in

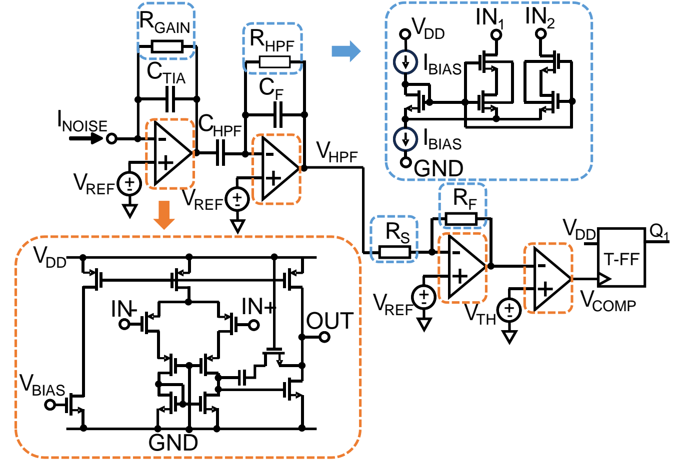

Fig. 11. RTN-based TRNG circuit designed in IHP SG13S 130 nm technology [17]. OPA and the pseudo resistor [35] designs indicated by dashed orange and blue rectangles. The circuit operates at a V_{DD} of 0.7V. Each OPA dissipates ≈ 24.7 nW, with a gain of 60 dB, a bandwidth of 153 kHz, and a phase margin of 45°. Also, C_{TIA} = 31.5 fF, C_{HPF} = 500 fF, and C_F = 100 fF. The circuit is designed for a HPF cut-off frequency of ≈1.7 kHz, with a total pass-band gain at the comparator input > 170 dB.

these conditions, the DC drift can lead to the potential saturation of the input gain stage, thus preventing any transition at the output of the comparator, leading to a completely unreliable design. To maximize the robustness to DC drift the designer should ensure that the output of the input gain stage for the reference DC component should be around the midpoint of the output voltage swing. Thus, a reliability aware design should trade between maximum amplitude at the input of the comparator (i.e. which translates to a lower t_{min} and higher tolerance to V_{TH} variations) and robustness to DC drift.

VII. Analysis and Discussion of Circuit-Level Constraints

Integrated circuit implementations increase the number of constraints that must be considered during the design process. The two critical aspects include the power consumption and the footprint on the chip that must both be minimized to meet the requirement of IoT and edge computing devices. Both the low-power and the minimal area occupation introduce additional non-trivial design trade-offs. For example, to minimize the power dissipation the circuit must operate in subthreshold with a low supply voltage. This suggests that amplifiers have a reduced dynamic range and results in detrimental impact on both the tolerance to DC drift and to variations. Moreover, the minimization of the footprint on the chip area aggravates the problem of variability that affects subthreshold circuit designs. An effective solution is to increase the transistor area (i.e., the standard deviation of the threshold voltage decreases with the $\sqrt{Area}$). The area constraints on the chip also limits the area of on chip capacitors (i.e., C_{HPF} < 1 pF), and thus sets a boundary for the HPF cut-off frequency. The use of higher HPF cut-off frequencies decreases the voltage amplitude at the input of the comparator and as consequence higher gains should be

employed, which in turn leads to overhead in the device footprint area and the power consumption.

A. Circuit simulation with 130 nm CMOS technology

An RTN-based TRNG circuit was designed using the SGS13 130 nm technology from IHP [17]. The circuit, shown in Fig. 11, was designed to operate with a single supply voltage of 0.7 V. Each operational amplifier (OPA) was designed as a dual stage with RC compensation and PMOS inputs to reduce the circuit injected noise (dashed orange enclosure in Fig. 11). As a result, the TIA input referred current noise has negligible impact on the overall input noise compared to the noise injected by the input test structures. To limit the capacitance value implemented on chip, a C_{HPF} of 500 fF was used. Resistors were implemented using the pseudo-resistor design from [35] as shown in Fig. 11 (dashed blue enclosures) to achieve high gain while limiting the circuit area. The total signal amplification gain was split into three stages to reduce the impact of the drift of the DC component. The first stage amplifies the signal so that a sufficient signal to noise ratio is provided as an input to an active HPF filter which filters out the DC component and further amplifies the signal. Finally, an additional inverting amplifier amplifies the output of the HPF filter to increase the amplitude at the input of the comparator. Increasing the gain after the HPF filter reduces the risk of saturating the output of the OPA due to drifts of the DC component.

B. Results of circuit-level transient noise simulations

By performing transient noise simulations of the circuit shown in Fig. 11, we qualitatively demonstrate the challenges that could arise at the circuit level. We would like to highlight the importance on design of the input amplifier gain stage in Fig. 12. Here, the circuit is provided with an RTN signal showing several instabilities, including drift of the DC component. The results show that when the gain of the input stage is optimized for a specific DC component, the circuit is able to correctly harness the entropy from the device. However, the drifts of the DC component in the input can easily saturate the OPA output. As shown in Fig. 12a, the circuit can still harness the $1/f^2$ noise component, however the $1/f$ one is lost. This represents one such worst case scenarios as the RTN capture and emission time constants also change over time in addition to the DC drift present in the RTN. We find that losing the $1/f$ noise component determines a drop in the output bitstream randomness (i.e., 8% drop in the NIST pass rate) in this example. In fact, by visual inspection the output of the T-FF remains stable for long periods of time, thus statistically biasing the output sequence. On the contrary, as suggested in Section VI.C, to optimize the tolerance to the drift of the DC component we designed the circuit so that the output of the input comparator is set to half of the voltage swing of the comparator. As shown in Fig. 12b, the circuit is able to harness both noise components despite the drift in the signal DC-level and to achieve a high randomness (i.e., 100% NIST tests pass rate).

Additional potential reliability limitations that could arise in the circuit level implementations can be connected to the dielectric material used to fabricate the entropy source device. For instance, we qualitatively analyzed the potential reliability issues due to small $\Delta I/I$. Among the different test structures that were measured in this work, the SiO_2-based structure showed the lowest $\Delta I/I$ among the three materials tested. A low $\Delta I/I$ implies that large gains should be employed in the input

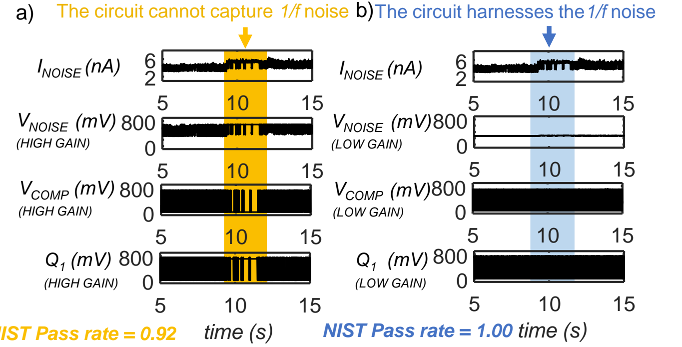

Fig. 12. Simulation outcomes for the circuit in Fig. 10 under an RTN signal with several instabilities from HfO_2-based test structure. Two R_{GAIN} values explored: a higher one in a) for maximum Signal-to-Noise Ratio (SNR), and a lower one in b). Higher gain enhances SNR but saturates the input stage when RTN signal's DC component drifts, hindering $1/f$ component exploitation (shaded orange region in a)), and resulting in decreased output randomness (see NIST test results).

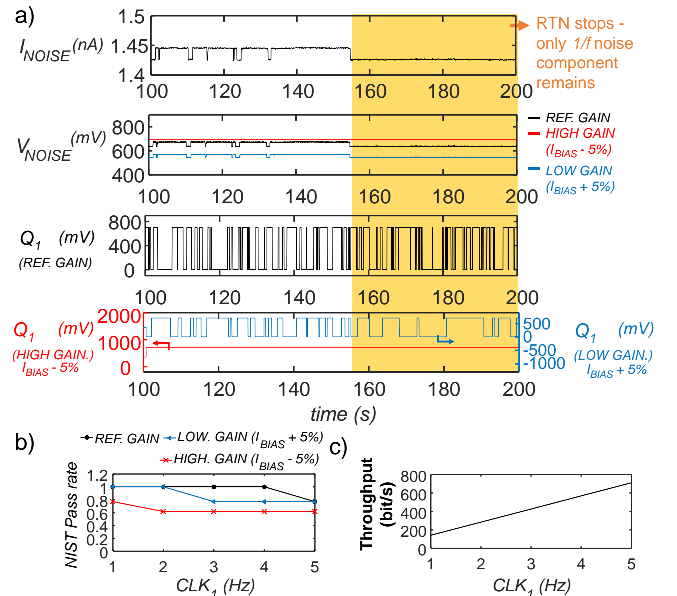

Fig. 13. Simulation outcomes for the circuit in Fig. 10 under temporary RTN signals from SiO_2-based device, with 3 R_{GAIN} values tested. Optimal gain (REF. GAIN) allowing the utilization of both $1/f^2$ and $1/f$ noise components. Lower and higher gains, achieved by adjusting I_{BIAS} in the pseudo resistor R_{GAIN} within ±5%. a) shows transient simulation results, while b) presents NIST test outcomes computed on a 14-bit NLFSR output sampled at different frequencies. The NLFSR, implemented using IHP standard cells, has an average power dissipation < 63 nW for throughputs up to 1Mbit/s at V_{DD} = 0.7V. NIST tests passed with p-value > 0.01. c), Circuit throughput at increasing CLK_1 frequencies.

amplification stage, making the circuit more sensitive to variations. For instance, we simulated the circuit considering a ± 5% variation in the I_{BIAS} current of the R_{GAIN} pseudo resistor and analyzed the randomness of the output bitstream. Variations on I_{BIAS} determine a change in the input stage gain, as shown in Fig. 13a. When considering the optimal gain at the reference I_{BIAS}, the output randomness is very high, see Fig. 13b, and the circuit is able to correctly harness the *1/f* noise component also when the $1/f^2$ noise component stops. A 5% decrease of I_{BIAS} saturates the output of the input gain stage, causing a complete malfunction of the circuit and a total loss of randomness. Conversely, with a 5% increase of I_{BIAS} the circuit can still operate, however with degraded performance in terms of randomness and throughput as shown in Fig. 13b, and c. In fact, the increase on I_{BIAS} translates to a lower input stage gain, which reduces the portion of the 1/f noise that can be effectively harnessed, determining a reduced switching activity at the output of the comparator that in turns limits the sampling frequency (CLK_1) and the output throughput. From this analysis it is clear that the input amplification stage gain is crucial for achieving RTN-based TRNG circuits reliability in spite of RTN instabilities and device-to-device variability. Future works should focus on proposing specific solutions to address potential drifts in the DC component of RTN signals. For example, adopting automatic gain control circuits [36] to automatically adjust the input amplifier gain for optimal entropy harnessing.

VIII. Conclusion

In this work, we assessed the reliability of an RTN-based TRNG by exploiting experimentally measured RTN signals on three distinct gate dielectrics: SiO_2, HfO_2, and h-BN. We demonstrated that when considering common RTN temporal instabilities, relying solely on the $1/f^2$ noise component leads to less robust TRNG designs. Designing the circuit to leverage also the *1/f* noise component yields more robust TRNG designs. Finally, we linked RTN signal properties and circuit parameters to the TRNG reliability, thus providing reliability aware design guidelines.

References

[1] A. Japa, M. K. Majumder, S. K. Sahoo, R. Vaddi, and B. K. Kaushik, "Hardware Security Exploiting Post-CMOS Devices: Fundamental Device Characteristics, State-of-the-Art Countermeasures, Challenges and Roadmap," *IEEE Circuits and Systems Magazine*, vol. 21, no. 3, pp. 4–30, 2021, doi: 10.1109/MCAS.2021.3092532.

[2] G. Rajendran, W. Banerjee, A. Chattopadhyay, and M. M. S. Aly, "Application of Resistive Random Access Memory in Hardware Security: A Review," *Advanced Electronic Materials*, vol. 7, no. 12, p. 2100536, 2021, doi: 10.1002/aelm.202100536.

[3] C. Pilato, S. Garg, K. Wu, R. Karri, and F. Regazzoni, "Securing Hardware Accelerators: A New Challenge for High-Level Synthesis," *IEEE Embedded Syst. Lett.*, vol. 10, no. 3, pp. 77–80, Sep. 2018, doi: 10.1109/LES.2017.2774800.

[4] N. Du, H. Schmidt, and I. Polian, "Low-power emerging memristive designs towards secure hardware systems for applications in internet of things," *Nano Materials Science*, vol. 3, no. 2, pp. 186–204, Jun. 2021, doi: 10.1016/j.nanoms.2021.01.001.

[5] Y. Pang, B. Gao, B. Lin, H. Qian, and H. Wu, "Memristors for Hardware Security Applications," *Advanced Electronic Materials*, vol. 5, no. 9, p. 1800872, 2019, doi: 10.1002/aelm.201800872.

[6] F. Rahman, B. Shakya, X. Xu, D. Forte, and M. Tehranipoor, "Security Beyond CMOS: Fundamentals, Applications, and Roadmap," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 25, no. 12, pp. 3420–3433, Dec. 2017, doi: 10.1109/TVLSI.2017.2742943.

[7] M. Lanza *et al.*, "Memristive technologies for data storage, computation, encryption, and radio-frequency communication," *Science*, vol. 376, no. 6597, p. eabj9979, Jun. 2022, doi: 10.1126/science.abj9979.

[8] J. Brown *et al.*, "Random-telegraph-noise-enabled true random number generator for hardware security," *Scientific Reports*, vol. 10, no. 1, Art. no. 1, Oct. 2020, doi: 10.1038/s41598-020-74351-y.

[9] C. Wen *et al.*, "Advanced Data Encryption using 2D Materials," *Advanced Materials*, vol. 33, no. 27, p. 2100185, 2021, doi: 10.1002/adma.202100185.

[10] S. Pazos *et al.*, "Hardware implementation of a true random number generator integrating a hexagonal boron nitride memristor with a commercial microcontroller," *Nanoscale*, p. 10.1039.D2NR06222D, 2023, doi: 10.1039/D2NR06222D.

[11] J. Kim *et al.*, "Nano-Intrinsic True Random Number Generation: A Device to Data Study," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 66, no. 7, pp. 2615–2626, Jul. 2019, doi: 10.1109/TCSI.2019.2895045.

[12] T. Zanotti, P. Pavan, and F. M. Puglisi, "Comprehensive physics-based RRAM compact model including the effect of variability and multi-level random telegraph noise," *Microelectronic Engineering*, p. 111886, Sep. 2022, doi: 10.1016/j.mee.2022.111886.

[13] S. Vecchi, P. Pavan, and F. M. Puglisi, "Defects Motion as the Key Source of Random Telegraph Noise Instability in Hafnium Oxide," in *ESSDERC 2022 - IEEE 52nd European Solid-State Device Research Conference (ESSDERC)*, Sep. 2022, pp. 368–371. doi: 10.1109/ESSDERC55479.2022.9947125.

[14] S. Vecchi, P. Pavan, and F. M. Puglisi, "Local electric field perturbations due to trapping mechanisms at defects: What random telegraph noise reveals," *Journal of Applied Physics*, vol. 133, no. 11, p. 114101, Mar. 2023, doi: 10.1063/5.0137245.

[15] S. Guo, R. Wang, D. Mao, Y. Wang, and R. Huang, "Anomalous random telegraph noise in nanoscale transistors as direct evidence of two metastable states of oxide traps," *Sci Rep*, vol. 7, no. 1, Art. no. 1, Jul. 2017, doi: 10.1038/s41598-017-06467-7.

[16] T. Zanotti *et al.*, "Reliability Analysis of Random Telegraph Noise-based True Random Number Generators," in *2023 IEEE International Integrated Reliability Workshop (IIRW)*, Oct. 2023, pp. 1–6. doi: 10.1109/IIRW59383.2023.10477697.

[17] "IHP BiCMOS." [Online]. Available: https://www.ihp-microelectronics.com/services/research-and-prototyping-service/mpw-prototyping-service/sigec-bicmos-technologies

[18] A. Ranjan *et al.*, "Spatially Controlled Generation and Probing of Random Telegraph Noise in Metal Nanocrystal Embedded HfO2 Using Defect Nanospectroscopy," *ACS Appl. Electron. Mater.*, vol. 4, no. 8, pp. 3909–3921, Aug. 2022, doi: 10.1021/acsaelm.2c00559.

[19] A. Ranjan *et al.*, "Random telegraph noise in 2D hexagonal boron nitride dielectric films," *Applied Physics Letters*, vol. 112, no. 13, p. 133505, Mar. 2018, doi: 10.1063/1.5022040.

[20] N. Vasileiadis, A. Mavropoulis, P. Loukas, G. Ch. Sirakoulis, and P. Dimitrakis, "Analysis of random telegraph noise in resistive memories: The case of unstable filaments," *Micro and Nano Engineering*, vol. 19, p. 100205, Jun. 2023, doi: 10.1016/j.mne.2023.100205.

[21] G. González-Cordero *et al.*, "Study of RTN signals in resistive switching devices based on neural networks," *Solid-State Electronics*, vol. 183, p. 108034, Sep. 2021, doi: 10.1016/j.sse.2021.108034.

[22] F. M. Puglisi and P. Pavan, "RTN analysis with FHMM as a tool for multi-trap characterization in HfOX RRAM," in *2013 IEEE International Conference of Electron Devices and Solid-state Circuits*, Jun. 2013, pp. 1–2. doi: 10.1109/EDSSC.2013.6628059.

[23] F. M. Puglisi and P. Pavan, "Factorial Hidden Markov Model analysis of Random Telegraph Noise in Resistive Random Access Memories," *ECTI Transactions on Electrical Engineering, Electronics, and Communications*, vol. 12, no. 1, Art. no. 1, Jan. 2014, doi: 10.37936/ecti-eec.2014121.170814.

[24] X. Chen *et al.*, "Modeling Random Telegraph Noise as a Randomness Source and its Application in True Random Number Generation," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 35, no. 9, pp. 1435–1448, Sep. 2016, doi: 10.1109/TCAD.2015.2511074.

[25] A. Mohanty, K. B. Sutaria, H. Awano, T. Sato, and Y. Cao, "RTN in Scaled Transistors for On-Chip Random Seed Generation," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 25, no. 8, pp. 2248–2257, Aug. 2017, doi: 10.1109/TVLSI.2017.2687762.
[26] M. Stipčević and Ç. K. Koç, "True Random Number Generators," in *Open Problems in Mathematics and Computational Science*, Ç. K. Koç, Ed., Cham: Springer International Publishing, 2014, pp. 275–315. doi: 10.1007/978-3-319-10683-0_12.
[27] P. Welch, "The use of fast Fourier transform for the estimation of power spectra: A method based on time averaging over short, modified periodograms," *IEEE Transactions on Audio and Electroacoustics*, vol. 15, no. 2, pp. 70–73, Jun. 1967, doi: 10.1109/TAU.1967.1161901.
[28] D. M. Fleetwood, "1/f Noise and Defects in Microelectronic Materials and Devices," *IEEE Transactions on Nuclear Science*, vol. 62, no. 4, pp. 1462–1486, Aug. 2015, doi: 10.1109/TNS.2015.2405852.
[29] K. S. Woo, Y. Wang, Y. Kim, J. Kim, W. Kim, and C. S. Hwang, "A Combination of a Volatile-Memristor-Based True Random-Number Generator and a Nonlinear-Feedback Shift Register for High-Speed Encryption," *Advanced Electronic Materials*, vol. 6, no. 5, p. 1901117, 2020, doi: https://doi.org/10.1002/aelm.201901117.
[30] E. Dubrova, "A List of Maximum Period NLFSRs," 166, 2012. Accessed: Nov. 12, 2020. [Online]. Available: http://eprint.iacr.org/2012/166
[31] X. Li, T. Zanotti, T. Wang, K. Zhu, F. M. Puglisi, and M. Lanza, "Random Telegraph Noise in Metal-Oxide Memristors for True Random Number Generators: A Materials Study," *Advanced Functional Materials*, p. 2102172, Apr. 2021.
[32] A. Rukhin *et al.*, "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications," National Institute of Standards and Technology, NIST Special Publication (SP) 800-22 Rev. 1a, Apr. 2010. doi: 10.6028/NIST.SP.800-22r1a.
[33] S. Kim, M.-S. Kim, Y. Lee, H.-D. Kim, Y.-K. Choi, and S.-J. Choi, "Low-Power True Random Number Generator Based on Randomly Distributed Carbon Nanotube Networks," *IEEE Access*, vol. 9, pp. 91341–91346, 2021, doi: 10.1109/ACCESS.2021.3091491.
[34] C. Chen, S. Li, and C. Song, "A 200 kb/s 36 µw True Random Number Generator Based on Dual Oscillators for IOT Security Application," *Electronics*, vol. 12, no. 10, Art. no. 10, Jan. 2023, doi: 10.3390/electronics12102332.
[35] A. Arnaud, R. Puyol, D. Hardy, M. Miguez, and J. Gak, "Bulk Linearization Techniques," in *2019 IEEE International Symposium on Circuits and Systems (ISCAS)*, May 2019, pp. 1–5. doi: 10.1109/ISCAS.2019.8702327.
[36] J. Hernandez, D. E. Garcia, and S. Mann, "HDR AGC Signal Optimization Applied to Audio," in *2020 IEEE SENSORS*, Oct. 2020, pp. 1–4. doi: 10.1109/SENSORS47125.2020.9278627.