IEEE Journal on Exploratory Solid-State Computational Devices and Circuits

Received 21 June 2023; revised 15 September 2023; accepted 22 September 2023.
Date of publication 29 September 2023; date of current version 26 October 2023.

Digital Object Identifier 10.1109/JXCDC.2023.3320056

True Random Number Generator Based on RRAM-Bias Current Starved Ring Oscillator

D. ARUMÍ[1], S. MANICH[1] (Member, IEEE), A. GÓMEZ-PAU[1] (Member, IEEE), R. RODRÍGUEZ-MONTAÑÉS[1], M. B. GONZÁLEZ[2], and F. CAMPABADAL[2]

[1]Departament d'Enginyeria Electrònica, Universitat Politècnica de Catalunya, 08028 Barcelona, Spain
[2]Institut de Microelectrònica de Barcelona, Centre Nacional de Microelectrònica, Consejo Superior de Investigaciones Científicas, 08193 Bellaterra, Spain

CORRESPONDING AUTHOR: D. ARUMÍ (daniel.arumi@upc.edu)

This work was supported by the Spanish MCIN/AEI/10.13039/501100011033 under Project PID2019-103869RB-C33. The work of M. B. González was supported by the Ramón y Cajal under Grant RYC2020-030150-I.

ABSTRACT This work presents a resistive random access memory (RRAM)-bias current-starved ring oscillator (CSRO) as true random number generator (TRNG), where the cycle-to-cycle variability of an RRAM device is exploited as source of randomness. A simple voltage divider composed of this RRAM and a resistor is considered to bias the gate terminal of the extra transistor of every current starved (CS) inverter of the ring oscillator (RO). In this way, the delay of the inverters is modified, deriving an unpredictable oscillation frequency every time the RRAM switches to the high resistance state (HRS). The oscillation frequency is finally leveraged to extract the sequence of random bits. The design is simple and adds low area overhead. Experimental measurements are performed to analyze the cycle-to-cycle variability in the HRS. The very same measurements are subsequently used to validate the TRNG by means of electrical simulations. The obtained results passed all the National Institute of Standards and Technology randomness tests (NIST) tests without the need for postprocessing.

INDEX TERMS Hardware security, non-volatile memory (NVM), random number generation, ring oscillator, resistive random access memory (RRAM), true random number generator (TRNG).

I. INTRODUCTION

Random number generators (RNGs) are commonly utilized in different application fields, such as engineering problem solving, statistical sampling, industrial simulations, gaming, communications, or cryptography [1]. In some of these applications sensitive data is managed, i.e., communication and cryptographic applications, where the use of PRNGs (pseudo-RNGs) is not recommended. In these applications, the generated random numbers must be truly random, fulfilling several statistical test requirements [2]. Thus, there is a deep interest in developing devices capable of harvesting entropy from physical phenomena so that the extracted random numbers fulfill such requirements. RNGs based on these physical sources of entropy are called true random number generators (TRNGs) [3]. TRNGs have become essential due to the growing security concern in the era of the Internet of Things (IoT). Different TRNGs have been proposed based on physical phenomena including thermal noise [4], random telegraph noise (RTN) [5], metastable elements [6], or current fluctuations [7]. In this article, resistive random access memory (RRAM) have also attracted the interest in the development of TRNGs. RRAMs present excellent properties in terms of switching speed, power consumption, scalability, endurance, and CMOS compatibility [10]. These properties together with the inherent nonvolatility of these devices motivated their initial use as memory devices [8], [9]. Furthermore, RRAMs have already been demonstrated for other applications such as neural networks [11] and digital logic [12]. However, massive production of RRAMs has been limited by their inherent stochastic features, such as probabilistic switching, inter- and intradevice variabilities [13], [14], RTN [15], and limited endurance. Significant research effort is currently devoted to overcome these limitations [16], [17], [18]. Nevertheless, these very same challenges provide interesting features for the development of hardware security applications [19], including physical unclonable functions (PUFs) and the mentioned TRNGs.

Regarding RRAM-based TRNGs, recent works have been focused on the extraction of random numbers by exploiting the cycle-to-cycle variability of RRAMs [20], the device-to-device variability [21], [22], the competition between paired devices [23], [24], [25], the combination of cycle-to-cycle and

© 2023 The Authors. This work is licensed under a Creative Commons Attribution 4.0 License.
For more information, see https://creativecommons.org/licenses/by/4.0/

device-to-device variability [26] and the occurrence of RTN [27], [28], [29]. All these RRAM-based TRNGs still suffer from some constraints, such as complexity in design, limited stability, need for postprocessing, or high cost.

This article presents an RRAM-bias current starved ring oscillator (CSRO) as TRNG. The cycle-to-cycle variability of an RRAM device is exploited as a source of randomness. A voltage divider composed of a single RRAM and a resistor is considered to bias the gate terminal of the extra pMOS transistor of every current starved (CS) inverter of the ring oscillator (RO). Before enabling the RO, the RRAM is forced to switch from low resistance state (LRS) to HRS. The cycle-to-cycle variability causes the RRAM to have a different equivalent resistance value in every switch from LRS to HRS, deriving thus a different oscillation frequency of the RO. This unpredictable oscillation frequency is exploited to extract a random bit by including a one-bit counter to the design. The circuit is simple, adding a low area overhead. Results based on experimental measurements confirm the feasibility of the proposal.

II. TRNG PROPOSAL

An RO is a well-known circuit composed of an odd number of regular inverters, whose outputs alternate between high and low voltage levels. The output of every inverter is in turn the input of the next one. The output of the last inverter is fed back to the first inverter. An example is illustrated in Fig. 1. One of the inverters is commonly replaced by a nand gate so that the extra input (EN) can enable/disable the RO. Due to the delay in every inverting stage, the RO spontaneously oscillates at a given frequency. Hence, ROs are exploited for a wide variety of applications, including hardware security primitives, such as PUFs and TRNGs.

By adding transistors to the regular inverter [Fig. 2(a)], a CS inverter is obtained. The extra transistors are used to control the drain current. The CS inverter in Fig. 2(b) includes an extra pMOS transistor. The one in Fig. 2(c) includes an extra nMOS transistor, whereas the CS inverter in Fig. 2(d) includes both pMOS and nMOS transistors. Concerning ROs, the delay of CS inverters can be controlled to adjust the frequency of oscillation. This adjustment can be obtained by the gate voltage of the additional transistors stacked in nMOS and/or pMOS networks. In the field of hardware security, CS inverters in ROs have been already proposed to counteract the effect of temperature in TRNGs [30] and to enhance the reliability against temperature and supply voltage variations in PUFs [31].

The proposed TRNG is based on CSRO where only an extra pMOS transistor has been included in every inverter, as shown in Fig. 3. This option has been selected to simplify the bias circuit to control the gate voltage of the extra transistors. The bias circuit is a voltage divider composed of an RRAM and a resistor (R_p), as illustrated in Fig. 4. The top electrode (TE) of the RRAM is connected to one of the terminals of the resistor ($V_{p'}$). The transmission gate isolates the voltage divider from the RO during the programming mode. When enabled (EN = 1), the transmission gate passes the voltage $V_{p'}$–V_p, which is in turn the gate terminal of the CS pMOS transistor of every inverter, as shown in Fig. 3. The voltage V_p depends on the HRS resistance value of the RRAM. Due to cycle-to-cycle variability, the equivalent resistance is unpredictable after every switch from LRS to HRS, inducing different frequencies of oscillation. The 1-bit counter allows the extraction of a random bit at the output of the circuit, as shown in Fig. 3. Although CSROs were proposed in [28] for TRNGs, that simulation work exploited RTN as the source of randomness.

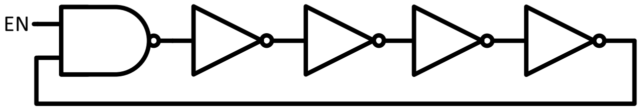

FIGURE 1. Five-stage RO with enable (EN) signal.

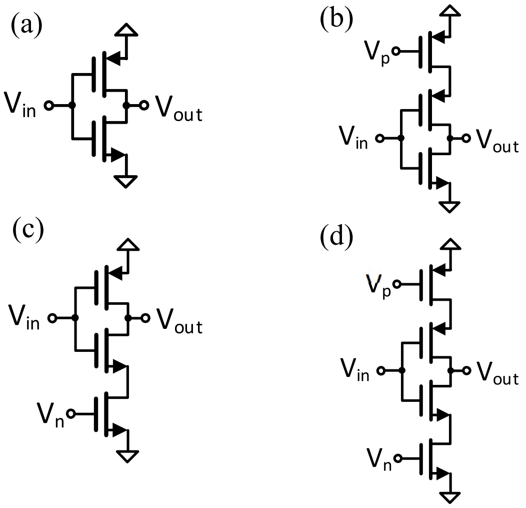

FIGURE 2. Schematic of (a) regular inverter, (b) CS inverter biasing pMOS transistor, (c) CS inverter biasing nMOS transistor, and (d) CS inverter biasing pMOS and nMOS transistor.

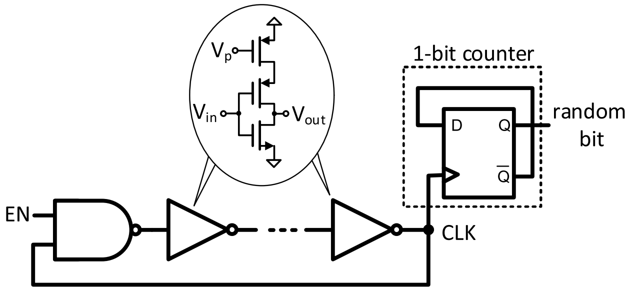

FIGURE 3. TRNG schematic.

The operation of the proposed TRNG is detailed next. An illustrative timing diagram summarizing the behavior of the TRNG is presented in Fig. 5.

1) Initially, the RRAM is in the HRS and the CSRO remains disabled (EN = 0).

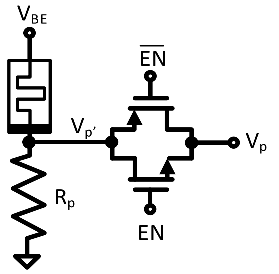

FIGURE 4. Bias generator based on an RRAM voltage divider (RRAM).

2) V_{READ1} is applied to the voltage divider (V_{BE}). Then, the CSRO is enabled during a certain period of time (PW). The unpredictable oscillation frequency of the CSRO depends on the particular (high) resistance value of the RRAM. The output of the flip-flop (1-bit counter) switches with every rising edge of the clock signal (CLK).
3) Once EN is low (CSRO disabled), a random 0/1 is obtained at the output of the TRNG (random bit). A logic 1 is obtained in the example in Fig. 5.
4) For a new random bit, an SET operation followed by a RESET operation is applied to the RRAM. (For simplicity, these operations have been omitted in Fig. 5.) Therefore, after applying this programming sequence the device is again in the HRS but with a different (high) resistance value due to the cycle-to-cycle variability.
5) The previous steps are then repeated to obtain the next random bit.

The CSRO must be enabled for a long time (PW) in comparison to the period of oscillation to ensure the randomness of the extracted sequence of bits. However, as the frequency of oscillation is high, PW can still be low enough to ensure a high throughput. During the normal operation of the RO, the voltage on the bottom electrode (BE) of the RRAM (V_{READ1}) must be appropriately selected to guarantee that the resistance state of the RRAM is not degraded, regardless the particular resistance value of the device. This issue is addressed in Section IV.

III. RRAM DEVICES AND MEASUREMENT SETUP

The RRAM devices considered throughout this work are TiN/Ti/HfO$_2$/W structures. The oxide thickness is 10 nm, and the area is 15×15 μm^2. More information about the fabrication process is given in [20]. The electrical characterization of the devices was performed using a Keysight B2912A Precision source/measure unit (SMU) and a Tektronix Arbitrary Function Generator (AFG3102). The experimental setup is shown in Fig. 6. The experiments were performed based on an equivalent configuration to the voltage divider proposed for the TRNG (Fig. 4). For the automation of the measurements, the instruments were connected to a computer via general purpose interface bus (GPIB) and controlled using MATLAB.

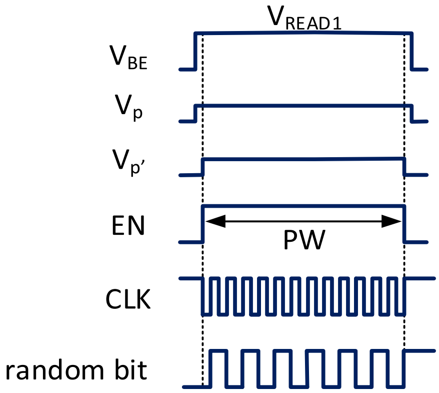

FIGURE 5. Timing diagram for the TRNG during the random bit generation stage.

Before carrying out the experiments to obtain the cycle-to-cycle variability of the RRAM, the device was assessed in dc and pulse mode. During this characterization, the HRS median was reported to be around 2.5 kΩ, while the LRS median was around 130 Ω. Therefore, there was around one order of magnitude between LRS and HRS.

IV. EXPERIMENTAL MEASUREMENTS

Once the electrical characteristics of the device were assessed, we conducted an experiment to extract the cycle-to-cycle variability of the device in HRS. We considered the same set-up previously presented in Fig. 6, including the voltage divider composed of an RRAM and a resistor (R_p). In this case, the purpose of the experiment was focused on measuring the cycle-to-cycle variability in HRS and its potential exploitation as a source of randomness. We considered the variability in HRS since it is higher than the one in LRS. In this experiment, we applied a long sequence of SET–READ1–RESET–READ2 pulses to obtain 10^6 resistance states in HRS. The timing diagram of the applied voltages is shown in Fig. 7. SET and RESET operations were required to switch the device from one state to the other (from HRS to LRS and LRS to HRS, respectively). The READ operation after RESET (READ1) was applied to measure the resistance state after the RESET operation. It must be pointed out that it is equivalent to the bias configuration of the voltage divider to be considered during the operation of the TRNG, i.e., when the RO is enabled, see Fig. 5. Finally, the READ operation after SET (READ2) was not strictly necessary and was only included for validation purposes. Therefore, we could read the state in LRS and thus check the behavior of the device along the experiment. According to Fig. 7, V_{RESET} was positive since RESET pulses were applied to the BE (V_{BE}) of the device by means of the function generator. Nevertheless, V_{SET} was also positive because SET pulses were applied to the TE (V_p) of the device by means of the SMU.

V_{READ1} was thoughtfully selected, assuming worst-case conditions for voltage drop estimation across RRAM, considering that $R_p = 4$ kΩ. For this purpose, we selected

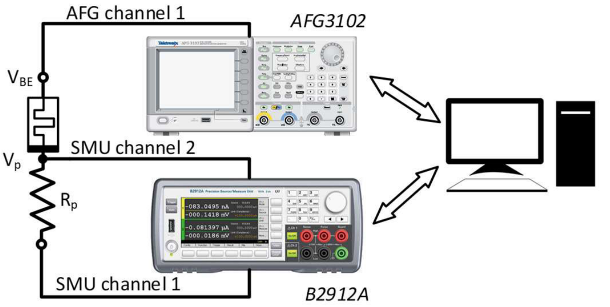

FIGURE 6. **Experimental setup.**

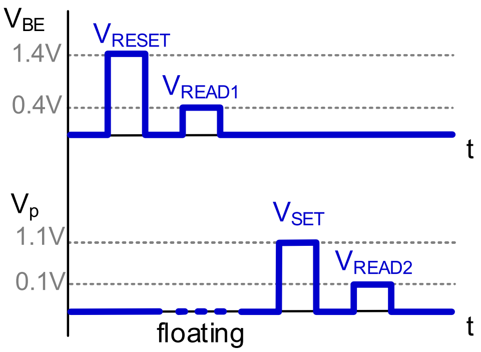

FIGURE 7. **Timing diagram used to extract a high number of resistance values in HRS based on the experimental setup from Fig. 6.**

$V_{\mathrm{READ1}} = 0.4$ V. In this way, the resistance state of the RRAM was not degraded, as we will discuss later. The histogram summarizing the results from the sequence of RESET–READ1–SET–READ2 pulses to obtain 10^6 resistance states in HRS is shown in Fig. 8(a). The plotted resistances are those measured during READ1. The corresponding cumulative probability plot is shown in Fig. 8(b). The resistance variability is slightly higher than one order of magnitude and follows a similar trend as reported in other works for similar devices [32]. This variability is exploited as a source of randomness for the proposed TRNG.

Another experiment was also conducted to demonstrate that the resistance state was not degraded during READ1. This experiment assessed the behavior of the device in pulse mode but applying two READ pulses after a RESET operation to measure the equivalent resistance of the device in HRS. These two READ pulses had different voltage amplitudes: the typical READ voltage (0.1 V) was applied first and next the worst-case scenario was applied ($V_{\mathrm{READ1}} = 0.4$ V). The results are illustrated in Fig. 9. It is observed that the resistance values are very similar in both cases, without noticeable degradation when a higher READ voltage was applied.

V. SIMULATION RESULTS

The proposed TRNG (Fig. 3) was designed for the STMicroelectronics 65-nm CMOS process. Electrical simulations of the circuit were subsequently performed with HSPICE. The RO included seven inverting stages. All the cells were based on transistors with standard V_T. nand gate (strength ×2) and D Flip-Flop (strength ×4) were standard cells provided by the hit-kit of the technology. The CS inverters (HS65_LS_CSIVX2) were based on an inverter provided also by the hit-kit (strength ×2), but modified to include the extra pMOS transistor. A summary of the cells considered in the design is shown in Table 1. The RRAM was emulated by a variable resistance so that the particular resistance was set according to the experiments obtained with the real device, as reported in Fig. 8. In fact, the sequence of equivalent resistance values was forced to follow the same order as they were obtained during the experiments.

TABLE 1. **Cells used in the CSRO.**

Cell	Number of cells	Unit area (μm^2)
HS65_LS_NAND2X2	1	2.08
HS65_LS_CSIVX2*	6	1.96
HS65_LS_DFPHQNX4	1	10.9

Throughout the simulations, the operating voltage (V_{DD}) of the TRNG was 0.7 V. The voltage applied to the voltage divider (V_{BE}) was $V_{\mathrm{READ1}} = 0.4$ V, the same value used during the experimental measurements and $R_P = 4$ kΩ. The relationship between the RRAM resistance and the induced frequency of oscillation is illustrated in Fig. 10. As expected, the higher the RRAM resistance, the lower the V_P, and as a result, the higher the oscillation frequency. The range of oscillation frequencies is higher than one order of magnitude within the range of RRAM resistances obtained during the experiments (red-shaded area in Fig. 10). The plot also represents the equivalent number of rising edges (N_{count}) for PW = 900 ns, i.e., the time interval the CSRO was enabled during the simulations.

VI. EVALUATION AND DISCUSSION

To assess the performance of the proposal, the National Institute of Standards and Technology randomness tests (NIST) (SP800-22) were used to evaluate the stochasticity of the bitstream [33]. The 1-bit bitstream was composed of 10^6 bits obtained from the simulations of the TRNG based on the resistance values extracted from the experimental results presented in Section IV. For each randomness test, a probability value (P-value) was returned and compared to the significance level to check whether the bitstream was random. A specific test was passed only when the resulting P-value was larger than the significance level (0.01), otherwise, it failed. The results are summarized in Table 2, including also the P-value. The obtained bitstream provided high randomness performance and passed all the NIST randomness tests. It is worth mentioning that no postprocessing was required to pass the tests.

The effect of temperature was also considered. The circuit was simulated for $T = 5$ °C and $T = 125$ °C. The RRAM measurements were obtained at room temperature.

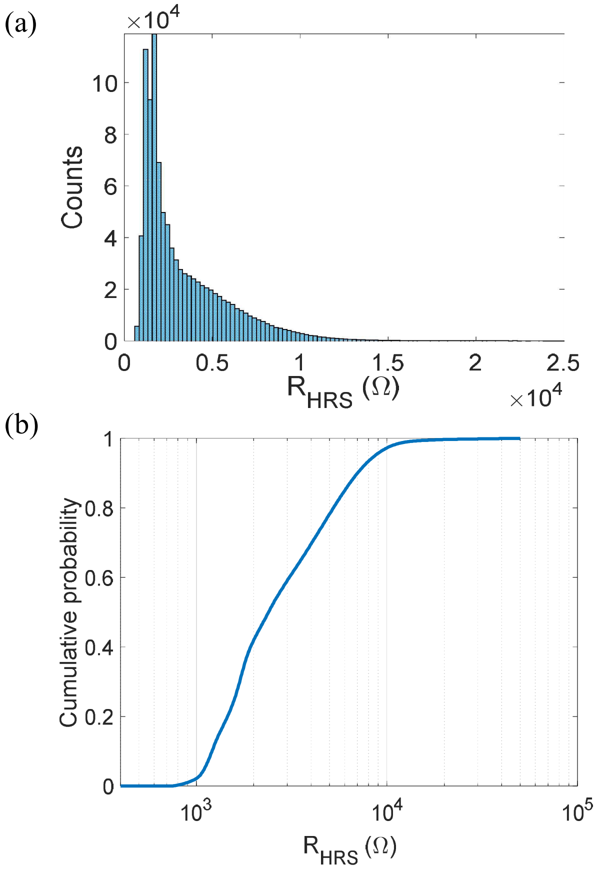

FIGURE 8. Experimental results for 10^6 resistance values in HRS. (a) Histogram plot. (b) Cumulative probability plot.

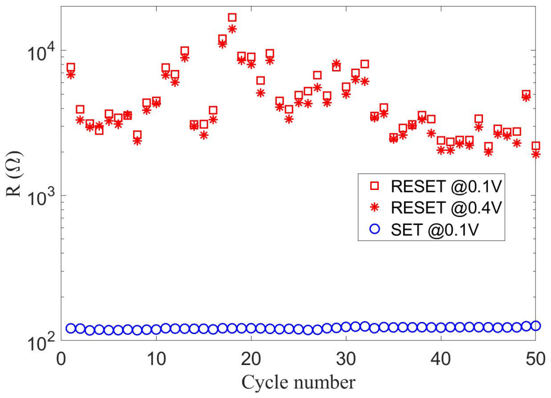

FIGURE 9. Equivalent resistance during successive pulsed SET and RESET operations. The resistance after RESET is measured at two consecutive READ voltages, first V_{READ} = 0.1 V, and then V_{READ} = 0.4 V.

The obtained bitstreams reported similar randomness properties and passed all the tests.

The pulse parameter (PW) was carefully chosen to ensure the randomness of the generated bits. PW should be kept low since it has a negative impact on throughput. Moreover, the time required to apply an SET and an RESET operation to the RRAM must also be considered to estimate the speed of the TRNG. In this article, the present implementation with the current experimental setup provides low throughput, but it is still sufficient for some encryption applications [27]. Nevertheless, speed is limited by the setup rather than the circuit proposal itself. In fact, RRAM devices have been proven to switch at a much faster speed (<10 ns) [34]. Furthermore, ROs implemented in lower technology nodes will result in higher oscillation frequencies, which in turn will allow decreasing PW. Hence, in an overall implementation, the proposed TRNG could easily provide a throughput in the order of Mbps.

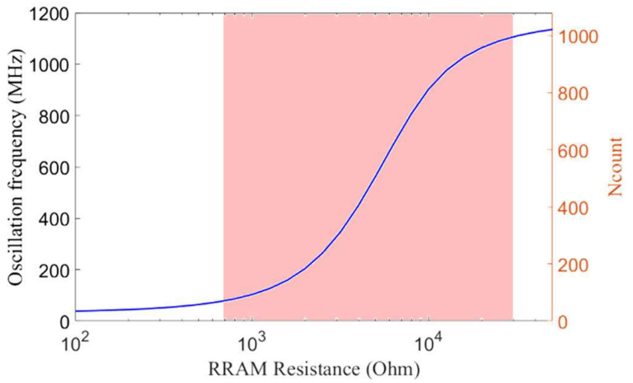

FIGURE 10. Oscillation frequency as a function of the RRAM resistance. The number of counts (N_{count}) is also shown considering PW = 900 ns.

TABLE 2. NIST SP800-22 test results when the *P*-value was larger than the significance level (0.01).

Test	P-value	Result
Frequency Test	0.18154	PASSED
Test For Frequency Within A Block	0.66757	PASSED
Runs Test	0.28542	PASSED
Test For The Longest Run Of Ones In A Block	0.03537	PASSED
Random Binary Matrix Rank Test	0.58403	PASSED
Discrete Fourier Transform Test	0.76202	PASSED
Non-Overlapping Template Matching Test	>0.04623	PASSED
Overlapping Template Matching Test	0.67856	PASSED
Maurer's Universal Statistical Test	0.53288	PASSED
Linear Complexity Test	0.97325	PASSED
Serial Test	>0.71161	PASSED
Approximate Entropy Test	0.49977	PASSED
Cumulative Sum (forward/backward) Test	>0.15081	PASSED
Random Excursions Test	>0.41702	PASSED
Random Excursions Variant Test	>0.03034	PASSED

In terms of area, the proposed circuit is simple and does not lead to significant area overhead. However, the area of the circuit (Table 1) will decrease with an implementation in a lower technology node. A similar reasoning can be applied to the bias generator circuit. The targeted RRAM, intended for research purposes, could be replaced by a smaller device (nm range instead of μm) in a final implementation of the TRNG so that it would not be the limiting component in terms of area.

During the enabling of the RO, RRAM is biased with a low voltage value, which could boost the appearance of RTN.

TABLE 3. Comparative analysis of RRAM-based TRNGs.

Work	Random source	Calibration free	# of RRAMs	RRAM integration	Required circuit	Throughput	NIST passed	Post-processing
[20]	Intra-device switching variability	Yes	1	Single cell	Comparator and counter	~Mbps	9/9	No
[21]	Probabilistic switching	No (median value of V_{SET})	1	1T-1R (7x7 array)	Comparator	N/A	11/15	No
[22]	Inter-device variability	Yes	2	2 Mbit array	Comparator	10 Kbps	10/10	XOR
[23]	Switching delay between devices	Yes	2	1T-1R	Comparator	0.16 Kbps	9/15	Von Neumann
[24]	Inter/intra-device switching variability	Yes	2	1x2 array	Comparator	~10 Mbps	12/15	Von Neumann
[25]	Inter/intra-device switching variability	Yes	2	Simulation	SR latch	10 Mbps	15/15	No
[26]	RRAM switching current	Yes	1	7x7 array	Comparator	N/A	12/15	XOR
[27]	RTN	No (Reference voltage for RTN)	1	Single cell	Comparator and D Flip-flop	1 Kbps	5/15	No
[28]	RTN	No (V_{CTRL} of the nMOS transistor)	1	1T-1R	Ring oscillator and D Flip-flop	~Mbps-Gbps	12/12	No
[29]	RTN	No (DACs Calibration to compensate offset)	2	Single cell	Comparator and DAC	40 Mbps	15/15	Von Neumann
This work	Intra-device switching variability	Yes	1	Single cell	RO and D-Flip-Flop	~Mbps	15/15	No

Charge trapping and detrapping are typically in the order of μs–ms, similar to the order of magnitude (or higher) than the target PW. RTN is a multilevel low-frequency noise, exploited by other proposals as source of randomness. Hence, in a potential context where RTN might influence the behavior of the proposed TRNG, it would add an extra source of variability in the oscillation frequency, which would be beneficial from the randomness point of view.

Regarding power consumption, the simplicity of the proposal makes it suitable for low-power applications within Internet of Things (IoT). However, in the present work, the energy related to the programming of the RRAM is much higher than recommended. This is due to the target devices, intended for research purposes since the resistance states are low (from hundreds of Ωs in LRS to a few kilo-ohms in HRs). This issue is not expected to be a limiting factor, since it has been demonstrated that RRAMs can consume only 0.1 pJ/bit during a write operation [35]. This limitation can be solved in a final implementation by selecting an RRAM device with higher resistance state values. On the other hand, the energy consumed during the bit generation is 3.64 pJ/bit, which is a competitive result in comparison with other RRAM-based TRNGs.

Device-to-device variability is not expected to influence the behavior of the proposed TRNG as long as such variability is not significantly higher than the corresponding cycle-to-cycle variability. Otherwise, R_p should be adjusted accordingly.

A further comparison with existing RRAM-based TRNGs can be found from Table 3. The column referred to as "NIST passed" reports the number of passed tests related to the number of applied tests. In some cases, it was not possible to apply all the NIST tests (15). Our proposed TRNG reports promising results according to the comparison presented in Table 3.

VII. CONCLUSION

This article exploits the cycle-to-cycle variability of an RRAM in HRS as the source of randomness for a TRNG. A voltage divider composed of a single RRAM device and a resistor is used to bias the gate terminal of the extra pMOS transistor of CS inverters of an RO. When the RRAM switches to the HRS it induces a different (random) oscillation frequency in the RO. A 1-bit counter is included in the design to extract the sequence of random bits.

Experimental measurements were performed to derive the cycle-to-cycle variability of a real device. These measurements were subsequently included in electrical simulations to validate the behavior of the TRNG. NIST tests were applied to assess the stochasticity of the random bits. The obtained bitstream passed all the NIST tests without the need for postprocessing. The proposed TRNG is simple, adds low area overhead, and could easily provide a throughput in the order of Mb/s in a final implementation.

REFERENCES

[1] H. Martin, P. Peris-Lopez, J. E. Tapiador, and E. S. Millan, "A new TRNG based on coherent sampling with self-timed rings," *IEEE Trans. Ind. Informat.*, vol. 12, no. 1, pp. 91–100, Feb. 2016, doi: 10.1109/TII.2015.2502183.

[2] V. Van der Leest, R. Maes, G.-J. Schrijen, and P. Tuyls, "Hardware intrinsic security to protect value in the mobile market," in *Proc. Inf. Secur. Solutions Eur. Conf.*, Brussels, Belgium, H. Reimer, N. Pohlmann, and W. Schneider, Eds. Wiesbaden, Germany: Springer Vieweg, Oct. 2014, pp. 188–198, doi: 10.1007/978-3-658-06708-3_15.

[3] B. Sunar, W. Martin, and D. Stinson, "A provably secure true random number generator with built-in tolerance to active attacks," *IEEE Trans. Comput.*, vol. 56, no. 1, pp. 109–119, Jan. 2007, doi: 10.1109/TC.2007.250627.

[4] M. Bucci, L. Germani, R. Luzzi, A. Trifiletti, and M. Varanonuovo, "A high-speed oscillator-based truly random number source for cryptographic applications on a smartcard IC," *IEEE Trans. Comput.*, vol. 52, no. 4, pp. 403–409, Apr. 2003, doi: 10.1109/TC.2003.1190581.

[5] R. Brederlow, R. Prakash, C. Paulus, and R. Thewes, "A low-power true random number generator using random telegraph noise of single oxide-traps," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, San Francisco, CA, USA, Feb. 2006, pp. 1666–1675, doi: 10.1109/ISSCC.2006.1696222.

[6] C. Tokunaga, D. Blaauw, and T. Mudge, "True random number generator with a metastability-based quality control," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2007, pp. 404–405.

[7] S. Yasuda, H. Satake, T. Tanamoto, R. Ohba, K. Uchida, and S. Fujita, "Physical random number generator based on MOS structure after soft breakdown," *IEEE J. Solid-State Circuits*, vol. 39, no. 8, pp. 1375–1377, Aug. 2004, doi: 10.1109/JSSC.2004.831480.

[8] H. Wu et al., "Resistive random access memory for future information processing system," *Proc. IEEE*, vol. 105, no. 9, pp. 1770–1789, Sep. 2017, doi: 10.1109/JPROC.2017.2684830.

[9] H.-S. P. Wong, H.-Y. Lee, S. Yu, Y.-S. Chen, Y. Wu, P.-S. Chen, B. Lee, F. T. Chen, and M.-J. Tsai, "Metal–oxide RRAM," *Proc. IEEE*, vol. 100, no. 6, pp. 1951–1970, Jun. 2012.

[10] D. Ielmini, "Resistive switching memories based on metal oxides: Mechanisms, reliability and scaling," *Semicond. Sci. Technol.*, vol. 31, no. 6, Jun. 2016, Art. no. 063002, doi: 10.1088/0268-1242/31/6/063002.

[11] D. Ielmini, "Brain-inspired computing with resistive switching memory (RRAM): Devices, synapses and neural networks," *Microelectron. Eng.*, vol. 190, pp. 44–53, Apr. 2018, doi: 10.1016/j.mee.2018.01.009.

[12] S. Kvatinsky, G. Satat, N. Wald, E. G. Friedman, A. Kolodny, and U. C. Weiser, "Memristor-based material implication (IMPLY) logic: Design principles and methodologies," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 22, no. 10, pp. 2054–2066, Oct. 2014, doi: 10.1109/TVLSI.2013.2282132.

[13] A. Chen and M.-R. Lin, "Variability of resistive switching memories and its impact on crossbar array performance," in *Proc. Int. Rel. Phys. Symp.*, Apr. 2011, pp. MY.7.1–MY.7.4.

[14] A. Bricalli, E. Ambrosi, M. Laudato, M. Maestro, R. Rodriguez, and D. Ielmini, "Resistive switching device technology based on silicon oxide for improved ON–OFF ratio—Part I: Memory devices," *IEEE Trans. Electron Devices*, vol. 65, no. 1, pp. 115–121, Jan. 2018, doi: 10.1109/TED.2017.2777986.

[15] G. González-Cordero, M. B. González, F. Campabadal, F. Jiménez-Molinos, and J. B. Roldán, "A new technique to analyze RTN signals in resistive memories," *Microelectron. Eng.*, vol. 215, Jul. 2019, Art. no. 110994, doi: 10.1016/j.mee.2019.110994.

[16] F. M. Simanjuntak, S. Chandrasekaran, C.-C. Lin, and T.-Y. Tseng, "Switching failure mechanism in zinc peroxide-based programmable metallization cell," *Nanosc. Res. Lett.*, vol. 13, no. 1, p. 327, Dec. 2018, doi: 10.1186/s11671-018-2743-7.

[17] X. D. Huang, Y. Li, H. Y. Li, Y. F. Lu, K. H. Xue, and X. S. Miao, "Enhancement of DC/AC resistive switching performance in AlOx memristor by two-technique bilayer approach," *Appl. Phys. Lett.*, vol. 116, no. 17, Apr. 2020, Art. no. 173504, doi: 10.1063/5.0006850.

[18] C.-W. Hsu, I.-T. Wang, C.-L. Lo, M.-C. Chiang, W.-Y. Jang, C.-H. Lin, and T.-H. Hou, "Self-rectifying bipolar $\mathrm{TaO}_x/\mathrm{TiO}_2$ RRAM with superior endurance over 10^{12} cycles for 3D high-density storage-class memory," in *Proc. Symp. VLSI Technol.*, Kyoto, Japan, 2013, pp. T166–T167.

[19] J. Rajendran, R. Karri, J. B. Wendt, M. Potkonjak, N. McDonald, G. S. Rose, and B. Wysocki, "Nano meets security: Exploring nanoelectronic devices for security applications," *Proc. IEEE*, vol. 103, no. 5, pp. 829–849, May 2015, doi: 10.1109/JPROC.2014.2387353.

[20] B. Yang, D. Arumí, S. Manich, Á. Gómez-Pau, R. Rodríguez-Montañés, M. B. González, F. Campabadal, and L. Fang, "RRAM random number generator based on train of pulses," *Electronics*, vol. 10, no. 15, p. 1831, Jul. 2021, doi: 10.3390/electronics10151831.

[21] J. Postel-Pellerin, H. Bazzi, H. Aziza, P. Canet, M. Moreau, V. D. Marca, and A. Harb, "True random number generation exploiting SET voltage variability in resistive RAM memory arrays," in *Proc. 19th Non-Volatile Memory Technol. Symp. (NVMTS)*, Durham, NC, USA, Oct. 2019, pp. 1–5, doi: 10.1109/NVMTS47818.2019.9043369.

[22] B. Cambou, D. Telesca, S. Assiri, M. Garrett, S. Jain, and M. Partridge, "TRNGs from pre-formed ReRAM arrays," *Cryptography*, vol. 5, no. 1, p. 8, Feb. 2021, doi: 10.3390/cryptography5010008.

[23] S. Balatti, S. Ambrogio, R. Carboni, V. Milo, Z. Wang, A. Calderoni, N. Ramaswamy and D. Ielmini, "Physical unbiased generation of random numbers with coupled resistive switching devices," *IEEE Trans. Electron Devices*, vol. 63, no. 5, pp. 2029–2035, May 2016, doi: 10.1109/TED.2016.2537792.

[24] T. Zhang, M. Yin, C. Xu, X. Lu, X. Sun, Y. Yang, and R. Huang, "High-speed true random number generation based on paired memristors for security electronics," *Nanotechnology*, vol. 28, no. 45, Nov. 2017, Art. no. 455202, doi: 10.1088/1361-6528/aa8b3a.

[25] M. S. Equbal, T. Ketkar, and S. Sahay, "Hybrid CMOS-RRAM true random number generator exploiting coupled entropy sources," *IEEE Trans. Electron Devices*, vol. 70, no. 3, pp. 1061–1066, Mar. 2023, doi: 10.1109/TED.2023.3241122.

[26] H. Aziza, J. Postel-Pellerin, H. Bazzi, P. Canet, M. Moreau, V. D. Marca, and A. Harb, "True random number generator integration in a resistive RAM memory array using input current limitation," *IEEE Trans. Nanotechnol.*, vol. 19, pp. 214–222, 2020, doi: 10.1109/TNANO.2020.2976735.

[27] C.-Y. Huang, W. C. Shen, Y.-H. Tseng, Y.-C. King, and C.-J. Lin, "A contact-resistive random-access-memory-based true random number generator," *IEEE Electron Device Lett.*, vol. 33, no. 8, pp. 1108–1110, Aug. 2012, doi: 10.1109/LED.2012.2199734.

[28] R. Govindaraj, S. Ghosh, and S. Katkoori, "CSRO-based reconfigurable true random number generator using RRAM," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 26, no. 12, pp. 2661–2670, Dec. 2018, doi: 10.1109/TVLSI.2018.2823274.

[29] J. Kim, H. Nili, N. D. Truong, T. Ahmed, J. Yang, D. S. Jeong, S. Sriram, D. C. Ranasinghe, S. Ippolito, H. Chun, and O. Kavehei, "Nano-intrinsic true random number generation: A device to data study," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 66, no. 7, pp. 2615–2626, Jul. 2019, doi: 10.1109/TCSI.2019.2895045.

[30] K. Wang, Y. Cao, C.-H. Chang, and X. Ji, "High-speed true random number generator based on differential current starved ring oscillators with improved thermal stability," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, May 2019, pp. 1–5, doi: 10.1109/ISCAS.2019.8702785.

[31] C. Q. Liu, Y. Cao, and C. H. Chang, "ACRO-PUF: A low-power, reliable and aging-resilient current starved inverter-based ring oscillator physical unclonable function," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 64, no. 12, pp. 3138–3149, Dec. 2017, doi: 10.1109/TCSI.2017.2729941.

[32] E. Salvador, M. B. Gonzalez, F. Campabadal, J. Martin-Martinez, R. Rodriguez, and E. Miranda, "SPICE modeling of cycle-to-cycle variability in RRAM devices," *Solid-State Electron.*, vol. 185, Nov. 2021, Art. no. 108040, doi: 10.1016/j.sse.2021.108040.

[33] L. E. Bassham III, A. L. Rukhin, J. Soto, J. R. Nechvatal, M. E. Smid, E. B. Barker, S. D. Leigh, M. Levenson, M. Vangel, D. L. Banks, and N. A. Heckert, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. SP 800-22 Rev. 1a, 2010.

[34] S. Yu and P.-Y. Chen, "Emerging memory technologies: Recent trends and prospects," *IEEE Solid State Circuits Mag.*, vol. 8, no. 2, pp. 43–56, Spring 2016, doi: 10.1109/MSSC.2016.2546199.

[35] F. Zahoor, T. Z. A. Zulkifli, and F. A. Khanday, "Resistive random access memory (RRAM): An overview of materials, switching mechanism, performance, multilevel cell (MLC) storage, modeling, and applications," *Nanosc. Res. Lett.*, vol. 15, no. 1, pp. 1–26, Dec. 2020.