HAL
open science

Resistive RAM SET and RESET Switching Voltage Evaluation as an Entropy Source for Random Number Generation

Hussein Bazzi, Jeremy Postel-Pellerin, Hassen Aziza, Mathieu Moreau, Adnan Harb

▶ **To cite this version:**

Hussein Bazzi, Jeremy Postel-Pellerin, Hassen Aziza, Mathieu Moreau, Adnan Harb. Resistive RAM SET and RESET Switching Voltage Evaluation as an Entropy Source for Random Number Generation. 2020 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), Oct 2020, Frascati, Italy. pp.1-4, 10.1109/DFT50435.2020.9250726 . hal-03504288

HAL Id: hal-03504288

https://hal.science/hal-03504288v1

Submitted on 29 Dec 2021

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Resistive RAM SET and RESET Switching Voltage Evaluation as an Entropy Source for Random Number Generation

Hussein Bazzi[1&2], Jeremy Postel-Pellerin[1], Hassen Aziza[1], Mathieu Moreau[1], Adnan Harb[3], Senior member, IEEE
[1]Aix-Marseille Univ, Univ Toulon, CNRS, IM2NP, Marseille, France, [2]Lebanese International University, Department of Electrical and Electronics Engineering, Beirut, Lebanon, [3]The International University of Beirut, Department of Electrical and Electronics Engineering, Beirut, Lebanon

***Abstract*—The intrinsic variability of the switching parameters in resistive memories has been a major wall that limits their adoption as the next generation memories. In contrast, this natural stochasticity can be beneficial for other applications such as Random Number Generators (RNGs). This paper presents two RNG approaches based on a 130nm HfO_2-based Resistive RAM (RRAM) memory array. The memory array is programmed with a voltage close to the median value of the SET (resp. RESET) voltage distribution to benefit from the SET (resp. RESET) voltage variability. In both cases, only a subset of the memory array is programmed, resulting in a stochastic distribution of cell resistance values. Resistance values are next converted into a bit stream and confronted to National Institute of Standards and Technology (NIST) test benchmarks.**

Keywords- Resistive memories, Resistive RAM (RRAM), Random Number Generator (RNG), Stochastic switching, Memory array.

I. INTRODUCTION

A True Random Number Generator (TRNG) is a device that generates random numbers from a physical process, rather than by means of an algorithm. These processes are, in theory, stochastic and completely unpredictable. Conventional TRNG have been demonstrated based on Random Telegraph Noise (RTN) that occurs in semiconductors and ultra-thin gate oxide films [1,2]. In the last decade, TRNG-based resistive-switching devices have been widely studied by several research groups [3,4]. RRAMs have been utilized in several TRNG applications due to their appealing characteristics, including intrinsic stochastic nature [5], immunity to radiation [6], high endurance, CMOS compatibility [7] and low power consumption [8]. It is worth noticing that in literature, the generic term RRAM is often used to generically refer to both Oxide Random Access Memory (OxRAM) and Conductive-Bridging Random Access Memory (CBRAM) [9]. In the rest of the paper, OxRAM technology will be considered.

OxRAM devices suffer from a significant variability that can be divided into two categories, Device to Device (D2D) and Cycle to Cycle (C2C) variabilities [10]. This downside is analyzed and explored in this paper at a memory array level to assess the potential to use OxRAMs as TRNGs. Two sources of entropy are considered, the first one is based on the SET switching voltage variability and the second one is based on the RESET switching voltage variability. In both cases, programming voltages close to the SET and RESET voltage median distributions are applied. In these conditions, half of the cells in the array are expected to be in Low Resistive State (LRS) and the other half in High Resistive State (HRS). Thus, a stochastic distribution of resistance values across the array is anticipated. These resistance values are converted into logical values to generate a random bit stream with a perfect balance between 0s and 1s during the OxRAM cell READ operation by carefully trimming the reading voltages/currents. As the proposed TRNG combines C2C and D2D variabilities within a memory array, it overcomes limitations of state of the art OxRAM-based TRNGs which are mainly based on a single memory cell [11-13]. Moreover, using a memory array instead of a single cell turns the random number generation process more reliable.

In section II, experimental results obtained from a memory array based on an OxRAM technology are presented. In section III, the random number generation process is detailed and random numbers are generated after both SET and RESET operations and converted into a bit stream. In Section IV, the bit stream is confronted to the National Institute of Standards and Technology (NIST) test bench. Finally, section V provides some concluding remarks.

II. OXRAM TECHNOLOGY

A. 1T1R memory cell

Devices used in our TRNG circuit are bipolar OxRAMs where bipolar voltage sweeps are required to switch the resistive element. An OxRAM consists of two metallic electrodes that sandwich a thin dielectric layer serving as a storage medium. This structure can be easily integrated in the Back-End-Of-Line (BEOL) in combination with advanced CMOS technologies. As reported in [14], the MIM structure is integrated on top of Metal 4 copper layer (Cu). A TiN Bottom Electrode (BE) is first deposited. Then, a 10nm-HfO_2/10nm-Ti/TiN stack is added. In this configuration one MOS transistor is serially connected to an OxRAM cell. The select transistor acts as current limiting device. It controls the amount of current flowing through the cell according to its gate voltage value in order to prevent memory cell damage during programming operations [15]. Fig. 1 (a) and (b) present typical 1T1R OxRAM I-V characteristics in linear scale. Based on these I-V curves,

the memory cell behavior can be seen as follows: after an initial electro-FORMING step (not presented here), the memory element can be reversibly switched between a High Resistance State (HRS) and a Low Resistance State (LRS). Resistive switching in an OxRAM corresponds to an abrupt change between HRS and LRS. This resistance change is achieved by applying specific biases across the 1T1R cell (i.e. V_{SET}, to switch from HRS to LRS and V_{RESET}, to switch from LRS to HRS). Fig. 1 (a) and (b) also highlight RESET and SET variabilities, here demonstrated after 7 consecutive RESET/SET operations applied to different cells (D2D in Fig. 1(a)) and to the same memory cell (C2C in Fig. 1(b)) across a memory array. Note that both D2D and C2C variabilities impact SET and RESET switching parameters. Table I presents the different voltage levels applied to the OxRAM cell during FORMING, RESET and SET operations. The whole experimental setup is based on a Keysight B1500 semiconductor parameter analyzer.

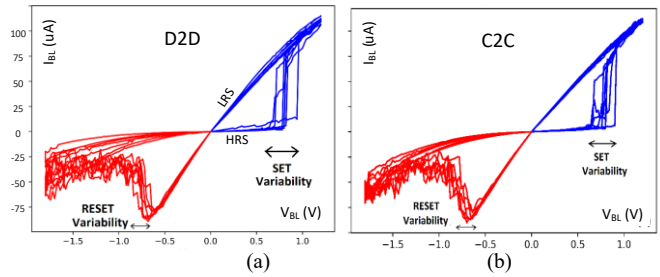

Fig. 1. I-V characteristics highlighting (a) D2D variability and (b) C2C variability. V_{SET} and V_{RESET} variabilities are highlighted in both cases.

TABLE I. STANDARD OPERATING VOLTAGES (CELL LEVEL)

	FORMING	RESET	SET	READ
WL	2V	4.5V	2V	4V
BL	2V	0V	1.2V	0.2V
SL	0V	1.8V	0V	0V

The proposed random number generation methodology exploits the HfO_2-based OxRAM variability (C2C and D2D) to generate a sequence of random bits. Indeed, HfO_2-based OxRAM technology suffers from stochastic switching. These statistical fluctuations are generally attributed to the formation/dissolution of a Conductive Filament (CF) between metallic electrodes [16-18]. The number of defects and the distance between traps within the CF in both SET and RESET states are considered as the main causes of variability [19].

B. 1T1R memory array

Fig. 2 (a) presents the TRNG circuit which is basically a classical 1T1R array. Memory cells are grouped to form eight 8-bit memory words. Word Lines (WL_X) are used to select the active row, Bit Lines (BL_X) are used to select active columns during a SET operation and Source Lines (SL_X) are used to RESET a whole memory word or an addressed cell. Fig. 2 (b) presents the layout view of the memory array. Due to the limited pin out of the probe card used in the experimental phase, only a 7x7 memory array is available for our experiments (subset of the 8x8 array). Based on this elementary memory array, the first step of the random number generation process is to extract SET and RESET switching voltage distributions over the array.

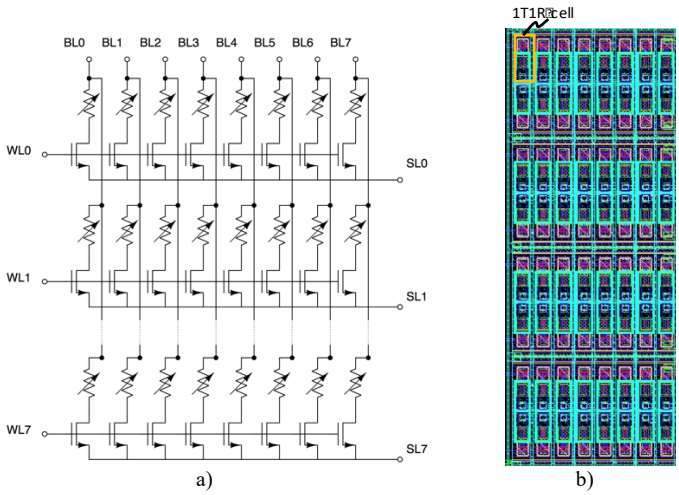

Fig. 2. (a) 8x8 OxRAM memory array and (b) corresponding layout view.

To extract the RESET distribution, the memory array is first SET. Then, memory cells are RESET one by one to extract the RESET voltage value referred to as V_{RESET}. Regarding V_{SET} distribution, the memory array is first RESET. Then, memory cells are SET one by one to extract the V_{SET} threshold. The process is repeated 1000 times for both V_{RESET} and V_{SET}. Fig. 3 (resp. Fig. 4) presents the resulting V_{RESET} (resp. V_{SET}) distribution.

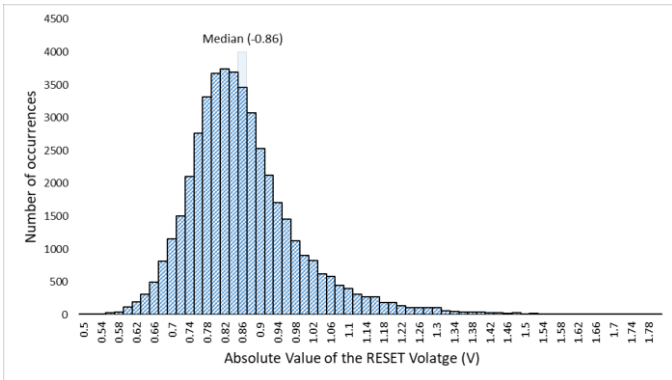

Fig. 3. RESET switching voltage (V_{RESET}) distribution obtained after 1000 SET/RESET cycles applied to the elementary memory array.

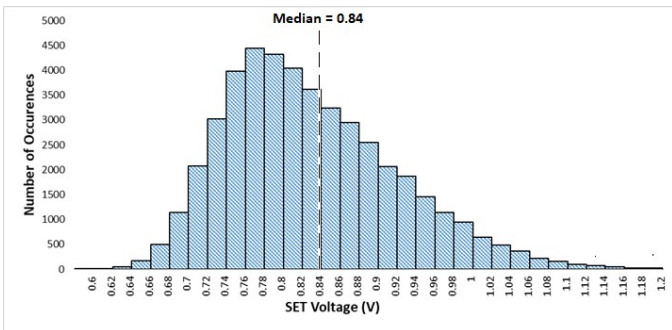

Fig. 4. SET switching voltage (V_{SET}) distribution obtained after 1000 RESET/SET cycles applied to the elementary memory array.

From these distributions, the median value of the RESET distribution referred to as V_{RESET_M} is extracted, as well as the median value of the SET distribution referred to as V_{SET_M}. Results are summarized in Table II.

TABLE II. V_{RESET}/V_{SET} DISTRIBUTION PARAMETERS

	Min	**Median**	Max
RESET	0.5 V	**-0.86 V**	1.8 V
SET	0.5 V	**0.84 V**	1.2 V

III. TRNG METHODOLOGY

Note that V_{RESET_M} and V_{SET_M} extraction is a key point in the presented random number generation methodology as these values will be used as the conventional SET and RESET voltages for the next programming operations.

A. RESET switching voltage-based RNG

This RN generation process consists in setting the whole memory array and resetting each cell individually with V_{RESET_M} = -0.86 V ("weak" RESET). As a result, some cells are switched to HRS, while others remain in LRS, resulting in a random distribution of resistance values. 100 runs are applied to the memory array to obtain a sufficiently large number of data (49x100). Fig. 5 presents an example of two 2D bitmaps obtained after two consecutive runs. Resistance values are represented by a greyscale from white (low values) to black (high values). Note that no spatial pattern reproduction has been detected after consecutive runs.

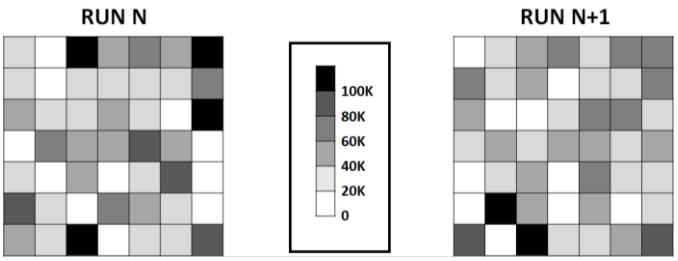

Fig. 5. Analog 2D bitmap (RESET) after Run N (left) and Run N+1 (right)

Fig. 6 presents the resistance distribution obtained after the weak RESET whose median value is equal to 32 kΩ. This median is used in order to convert resistance values into a stream of bits presenting a perfect balance between '0' and '1'. Despite external (temperature, etc.) or internal variations (degradation, etc.) the 50% ratio of '1' cells (and thus of '0' cells) has to be ensured. To this aim, real time voltage tracking techniques such as the one presented in [20] can be used. Indeed, NIST tests require an equal parity between '0' and '1'. To convert resistance values into '0' and '1', all values lower than R_M = 32 kΩ (dashed line in Fig. 6) are associated with a '1' logical state while all higher values are associated with a '0' logical state.

The reading circuitry which basically consists in a simple biasing circuit with its output connected to a comparator is in charge of the distribution split [21]. Thus, the analog bitmaps presented in Fig. 5 are turned into logical bitmaps presented in Fig. 7. At run N we obtain 29 bits at '1' level (and thus 20 bits at '0' level) and at run N+1 we obtain 23 bits at '1' level (and thus 26 bits at '0' level). Moreover, between the two presented runs 21 cells out of the 49 have changed their state and no systematic binary pattern has been observed between two consecutive runs.

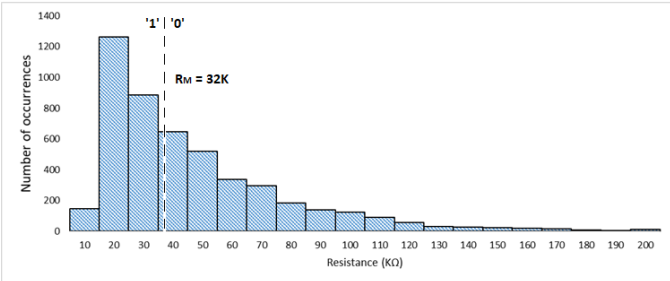

Fig. 6. Resistance distribution obtained after 100 consecutive memory array runs with a RESET value equals to V_{RESET_M} (-0.86 V).

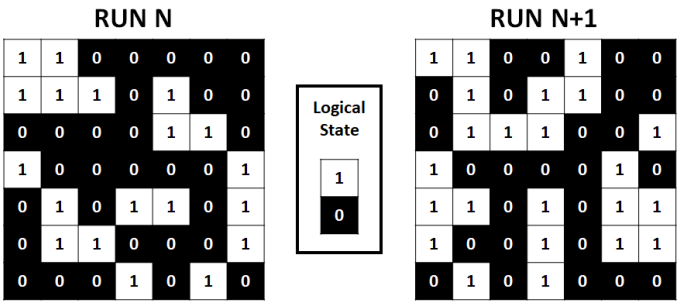

Fig. 7. Digital 2D bitmap (RESET) after Run N (left) and Run N+1 (right)

B. SET switching voltage-based RNG

In this configuration, the RN generation process consists in resetting the whole memory array and setting each cell individually with V_{SET_M} = 0.84 V ("weak" SET). This study was reported in a previous work [22] where the SET voltage variability was exploited for RNG. Here also, some cells are switched to LRS state, while others remain in HRS state, resulting in a random distribution of resistance values. However, the resistance dispersion is larger. Fig. 8 presents an example of two 2D bitmaps obtained after two consecutive runs. Fig. 9 presents the resistance distribution whose median value is equal to 145 kΩ with values ranging from 10 kΩ to 1 MΩ. To convert resistance values into '0' and '1', all values lower than R_M = 145 kΩ (dashed line of Fig. 9) are associated with a '1' logical state while all higher values are associated with a '0' logical state. Logical bitmaps are presented in Fig. 10. One can notice that at run N we obtain 28 bits at '1' level (and thus 21 bits at '0' level) and at run N+1 we obtain 28 bits at "1" level (and thus 21 bits at "0" level). Moreover, between the two presented consecutive runs, 13 cells out of the 49 have changed their state. Also, no systematic pattern is visible between the two runs.

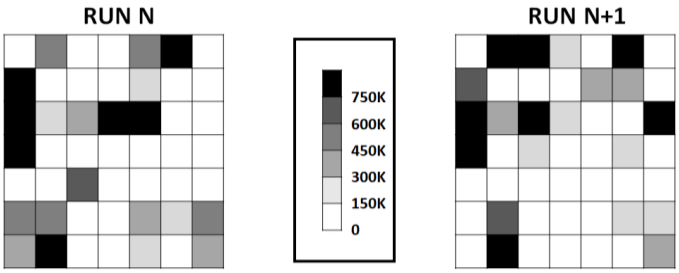

Fig. 8. Analog 2D bitmap (SET) after Run N (left) and Run N+1 (right)

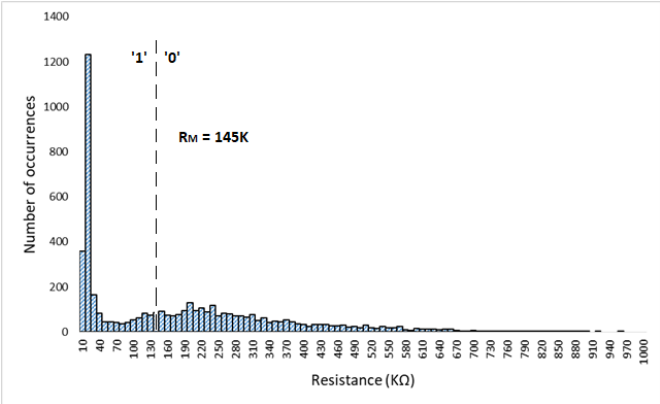

Fig. 9. Resistance distribution after 100 consecutive memory array runs (SET) [22]

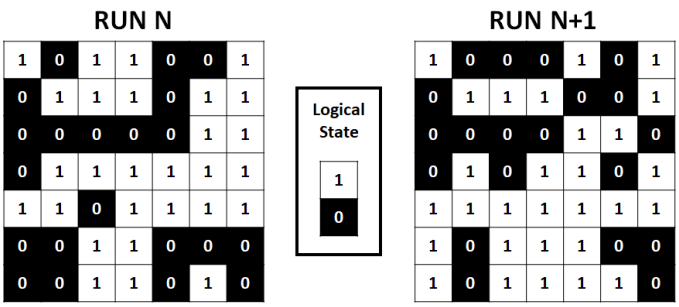

Fig. 10. Digital 2D bitmap (SET) after Run N (left) and Run N+1 (right)

IV. NIST Test Suite Results

The random numbers (4.9 kbits) generated after 100 runs and extracted from distributions presented in Fig. 6 (obtained after weak RESET) and Fig. 9 (obtained after weak SET) are verified against a statistical test suite. The statistical calculation is performed based on the NIST test suite for random and pseudorandom number generators for cryptographic applications [23]. For the distribution obtain after a weak RESET, the bit stream passes 9 NIST tests over 15 (see Table III). For the distribution obtained after a weak SET, the bit stream passes 11 NIST tests over 15 (see Table IV). It should be noted that these results are obtained without any post-processing step.

Tests 05-Binary Matrix Rank, 08-Overlapping Template Matching, 09-Maurer's Universal Statistical and 10-Linear Complexity are failed for both RESET and SET distributions. Indeed, these tests need a larger number of bits as recommended in [23]. Test 12-Approximate Entropy checks the frequency of all possible overlapping m-bit patterns across the entire sequence. The purpose of the test is to compare the frequency of overlapping blocks of two consecutive/adjacent lengths (m and m+1) against the expected result for a random sequence, ensuring the quality of the random number sequence. Only the SET switching voltage-based bit stream passes this test (p-value > 0.01). Same goes for test 6-Discrete Fourier Transform or DFT used to detect periodic features (i.e. repetitive patterns that are near each other).

TABLE III. NIST TEST SUITE RESULTS AFTER WEAK RESET

Test	p-value	Result
01-Frequency	0.8639	**Pass**
02-Frequency within a block	0.0872	**Pass**
03-Runs	0.7314	**Pass**
04-Longest Run of ones in a block	0.2693	**Pass**
05-Binary Matrix Rank	-	Fail
06-Discrete Fourier Transform	-	Fail
07-Non-Overlapping Template	0.5209	**Pass**
08-Overlapping Template Matching	-	Fail
09-Maurer's Universal Statistical	-	Fail
10-Linear Complexity	-	Fail
11-Serial	0.4781	**Pass**
12-Approximate Entropy	-	Fail
13-Cumulative Sums	0.1627	**Pass**
14-Random Excursions	0.3540	**Pass**
15-Random Excursions Variant	0.0726	**Pass**
Global NIST Score		**9/15**

TABLE IV. NIST TEST SUITE RESULTS AFTER WEAK SET

Test	p-value	Result
01-Frequency	0.1736	**Pass**
02-Frequency within a block	0.6711	**Pass**
03-Runs	0.8157	**Pass**
04-Longest Run of ones in a block	0.9077	**Pass**
05-Binary Matrix Rank	-	Fail
06-Discrete Fourier Transform	0.8623	**Pass**
07-Non-Overlapping Template	0.9970	**Pass**
08-Overlapping Template Matching	-	Fail
09-Maurer's Universal Statistical	-	Fail
10-Linear Complexity	-	Fail
11-Serial	0.4921	**Pass**
12-Approximate Entropy	0.9999	**Pass**
13-Cumulative Sums	0.3248	**Pass**
14-Random Excursions	0.4072	**Pass**
15-Random Excursions Variant	0.5929	**Pass**
Global NIST Score		**11/15**

A. *Comparison and Discussion*

Table V shows a comparison between the two proposed methods. The comparison is based on five parameters including NIST test result, resistance median distribution, expected energy/cell, expected bit-rate and the use of a post-processing step. The resistance distribution median value for RESET (32 kΩ) is lower than the SET one (145 kΩ). This difference has a straight impact on the energy consumption during the read operation preceding the bit stream generation. Thus, assuming that the RNG is properly configured (weak SET and weak RESET operation achieved and threshold resistances properly extracted), the energy/cell during RNG use is evaluated to 0.125 fJ and 0.027 fJ after weak RESET and weak SET respectively (values computed for a 100ns read pulse at 0.2V considering the average post weak RESET and post weak SET

resistances). Regarding the expected bit-rate, it has been demonstrated that read time in the 10ns order can be achieved for hafnium oxide devices resulting in bit rate in the order of 100 Mb/s [24]. Finally, the proposed RNGs do not include post-processing circuits such as XOR gates [25] and thus, can be improved in terms of randomness quality.

TABLE V. COMPARISON BETWEEN THE TWO PROPOSED METHODS

	NIST Results	Median Resistance	Energy/cell (fJ)	Bit-rate (Mb/s)	Post-processing
RESET	9	32 kΩ	0.125	100	No
SET	11	145 kΩ	0.027	100	No

From a physical point of view, generally, the HRS is more affected by switching variability, because the applied negative voltage results in a partial depletion of defects from the CF. Any variation in the conduction path and in the energy barrier impacts exponentially the resistance, therefore the statistical variations of HRS resistance are relatively large. Moreover, the resistance cumulative distributions slightly increases with V_{RESET}, as previously demonstrated by experiments and simulations of HfOx-based RRAM [26]. On the other hand, resistance fluctuations in the LRS are generally due to geometrical variations in the CF cross section, which affect LRS resistance only linearly resulting in tighter resistance distributions. Regarding randomness, no correlation with variability is observed as the weak SET programming approach produce better randomness than the weak RESET programming approach.

V. CONCLUSION

The proposed TRNG is implemented based on an elementary array of 1T1R OxRAM cells. Based on two programming method exploiting weak RESET and weak SET resistance distributions, it is possible to obtain random numbers. However, it has been demonstrated that the capability to produce randomness is higher for weak SET resistance distributions compared to weak RESET resistance distributions. These results have been confirmed after NIST tests. Indeed, the obtained bit streams have passed 9 and 11 NIST tests over 15 without any post-processing step for RESET and SET respectively.

ACKNOWLEDGMENT

The authors wish to acknowledge the support from Aix-Marseille University, and Lebanese International University.

REFERENCES

[1] R. Brederlow, et al., “A low-power true random number generator using random telegraph noise of single oxide-traps,” in ISSCC Tech. Dig., San Francisco, CA, USA, 2006, pp. 1666-1675.

[2] D. Lelmini, et al., “Resistance-Dependent Amplitude of Random Telegraph-Signal Noise in Resistive Switching Memories,” Applied Physics Letters, vol. 96, no. 5, 2010, p. 053503.

[3] Y. Wang, et al., “A novel true random number generator design leveraging emerging memristor technology,” in Proc. GLSVLSI, Pittsburgh, PA, USA, 2015, pp. 271-276.

[4] S. Sahay, et al., “Recent trend in hardware security exploiting hybrid CMOS-resistive memory circuits” in Semiconductor Science and Technology, vol. 32, no. 12, 2017, pp. 123001.

[5] V. Van der Leest, et al., “Hardware intrinsic security to protect value in the mobile market. ISSE 2014 Securing Electronic Business Processes (Springer Vieweg, Wiesbaden, 2014).

[6] Y. Wang, et al., "Highly Stable Radiation-Hardened Resistive-Switching Memory," in IEEE Electron Device Letters, vol. 31, no. 12, pp. 1470-1472, Dec. 2010.

[7] D. Ielmini, et al., "Physical modeling of voltage-driven resistive switching in oxide RRAM," 2012 IEEE International Integrated Reliability Workshop Final Report, South Lake Tahoe, CA, 2012, pp. 9-15.

[8] C. Cagli, et al., "Study of the Energy Consumption Optimization on RRAM Memory Array for SCM Applications," 2017 IEEE International Memory Workshop (IMW), Monterey, CA, 2017, pp. 1-4.

[9] H. Wang, et al., “Overview of Resistive Random Access Memory (RRAM): Materials, Filament Mechanisms, Performance Optimization, and Prospects,” Rapid Research Letters, vol. 13, no. 9, 2019, p. 1900073.

[10] A. Fantini, et al., “Intrinsic switching variability in HfO2 RRAM,” in Proc. IMW, Monterey, CA, 2013, pp. 30-33.

[11] S. Balatti, et al., “True random number generation by variability of resistive switching in oxide-based devices,” IEEE J. Emerg. Sel. Topics Circuits Syst., vol. 5, no. 2, pp. 214-221, June 2015.

[12] S. Sahay, et al., "OxRAM RNG Circuits Exploiting Multiple Undesirable Nanoscale Phenomena," in *IEEE Transactions on Nanotechnology*, vol. 16, no. 4, pp. 560-566, July 2017.

[13] H. Jiang, et al., “A novel true random number generator based on a stochastic diffusive memristor,” Nature communications, vol. 8, p. 882, Oct. 2017.

[14] G. Molas, et al., “Resistive Memories (RRAM) Variability: Challenges and Solutions,” *ECS Transactions*, vol. 86, no. 3, pp. 35-47, 2018.

[15] A. Grossi, et al., “Experimental Investigation of 4-kb RRAM Arrays Programming Conditions Suitable for TCAM,” *IEEE Trans. VLSI Syst.*, vol. 26, no. 12, pp. 2599-2607, Dec. 2018.

[16] S. Larentis, et al., “Resistive switching by voltage-driven ion migration in bipolar RRAM – Part II: Modeling”, in *IEEE Trans. Electron Devices*, vol. 59, no. 9, pp. 2468-2475, Jun. 2012.

[17] E. Miranda, “Compact model for the major and minor hysteretic I-V loops in nonlinear memristive devices”, in *IEEE Transactions on Nanotechnology*, vol. 14, no. 5, pp. 787-789, July 2015.

[18] L. Larcher, et al., “Microscopic understanding and modeling of HfO_2 RRAM device physics”, in *Proc. IEDM*, San Francisco, CA, USA, 2012, pp. 20.1.1-20.1.4.

[19] F. M. Puglisi, et al., “Bipolar Resistive RAM Based on HfO2: Physics, Compact Modeling, and Variability Control,” *IEEE J. Emerg. Sel. Topics Circuits and Syst.*, vol. 6, no. 2, pp. 171-184, June 2016.

[20] W. H. Choi et al., “A magnetic tunnel junction based true random number generator with conditional perturb and real-time output probability tracking,” in Proc. IEEE Int. Electron Devices Meeting (IEDM), Dec. 2014, pp. 12.5.1–12.5.4.

[21] H. Aziza, et al., “A built-in self-test structure (BIST) for resistive RAMs characterization: Application to bipolar OxRRAM. Solid-State Electronics”, 103, pp.73-78, 2015.

[22] J. Postel-Pellerin, et al., "True Random Number Generation Exploiting SET Voltage Variability in Resistive RAM Memory Arrays." 2019 19th Non-Volatile Memory Technology Symposium (NVMTS), In press.

[23] A. Rukhin, et al., “A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications,” *Nat. Inst. Standards Technol.*, Gaithersburg, MD, USA, Pub. 800-22, 2001.

[24] Boubacar Traore. Investigation of HfO2-based resistive RAM cells by electrical characterization and atomistic simulations. Micro and nanotechnologies/Microelectronics. Université Grenoble Alpes, 2015.

[25] D. Kaya, et al.., “Random Number Generators Based on Irregular Sampling and Fibonacci–Galois Ring Oscillators.” IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 66, no. 10, 2019, pp. 1718–1722.

[26] S. Ambrogio, et al., “Statistical fluctuations in HfOx resistive- switching memory (RRAM): Part I – Set/Reset variability,” IEEE Trans. Electron Devices, vol. 61, no. 8, pp. 2912–2919, Aug. 2014.