True Random Number Generator Integration in a Resistive RAM Memory Array Using Input Current Limitation

Hassen Aziza, Jeremy Postel-Pellerin, Hussein Bazzi, Pierre Canet, Mathieu Moreau, Vincenzo Della Marca, Adnan Harb

True Random Number Generator Integration in a Resistive RAM Memory Array using Input Current Limitation

H. Aziza, J. Postel-Pellerin, H. Bazzi, P. Canet, M. Moreau, V. Della Marca, A. Harb, *Member, IEEE*

***Abstract*— A novel True Random Number Generator circuit fabricated in a 130nm HfO_2-based resistive RAM process is presented. The generation of the random bit stream is based on a specific programming sequence applied to a dedicated memory array. In the proposed programming scheme, all the cells of the memory array are addressed at the same time while the current provided to the circuit is limited to program only a subset of the memory array, resulting in a stochastic distribution of cell resistance values. Some cells are switched in a low resistive state, other cells are slightly programmed to reach an intermediate resistance state, while the remaining cells maintain their initial high resistance state. Resistance values are next converted into a bit stream and confronted to National Institute of Standards and Technology (NIST) test benchmarks. The generated random bit stream has successfully passed twelve NIST tests out of fifteen. Compared to state-of-the-art resistive RAM-based true random number generators, our proposed methodology is the first one to leverage on programming current limitation at a memory array level.**

***Index Terms*— True Random Number Generator, TRNG, stochastic switching, memristor, OxRAM, RRAM.**

I. Introduction

True Random Number Generators (TRNGs) are incorporated in many data encryption systems in order to generate non-predictable data, which can be used as cryptographic keys [1]. TRNG exploits a physical entropy source to generate random numbers, rather than by means of an algorithm [2]. Such generators are often based on Random Telegraph Noise (RTN) that occurs in semiconductors and ultra-thin gate oxide films [3]. Over the last few years there has been a lot of activity across research groups proposing efficient TRNG based on resistive-switching devices [4-6]. Among these devices, bipolar oxide-based RAM (so-called OxRAM) have shown interesting properties [7-12].

OxRAM devices intrinsically suffer from significant spatiotemporal variability [13-15]. Switching parameters vary from device to device and cycle to cycle [16, 17]. This inherent drawback of the technology is exploited in this paper to propose a cost-efficient TRNG. In this context, this work presents a novel true random number generation methodology based on Input Current Limitation (ICL) of an OxRAM memory array when a global programming is performed. During a standard OxRAM cell SET operation, a single cell is addressed and the current flowing through the selected cell is limited, usually by a select transistor in a 1T1R (1 Transistor 1 Resistor) configuration to a value high enough to program the cell. In our approach, all the cells of the memory array are addressed during a global SET operation while the available current for the array is limited, resulting in a stochastic distribution of resistance values. Afterward, resistance values are converted into logical values to generate a random bit stream. To the authors' knowledge, this is the first work which presents an integrated compact OxRAM-based TRNG based on ICL at a memory array level during a global SET operation.

The proposed TRNG overcomes limitations of state of the art OxRAM-based TRNG which are mainly based on a single memory cell [6, 7, 18-20]. Using a whole memory array to generate random numbers combine the temporal effect of cycle to cycle variability and the spatial effect of device to device variability. Besides, as the proposed methodology relies on a whole memory array, instead of a single cell, the proposed TRNG is turned more reliable. A post-processing can be added to improve the entropy of the random bit stream as already proposed in previous studies found in the literature [20-23]. In our case, only a XOR operation is applied to the memory array bits to generate a single bit response. Indeed, as the TRNG circuit is represented by a standard memory array, only conventional decoding and reading circuits are required for its operation.

The rest of the paper is organized as follows. In section II, the used OxRAM technology is presented with experimental results obtained from a memory array. In section III, the true random number generation methodology is developed and experimental results are provided. National Institute of Standards and Technology (NIST) test results are given in section IV. Finally, section V provides some concluding remarks.

Manuscript submitted July xx, 2019.
H. Aziza, J. Postel-Pellerin, P. Canet, M. Moreau and V. Della Marca are with the Aix Marseille Univ, Université de Toulon, CNRS, IM2NP, Marseille, France (e-mail: hassen.aziza@univ-amu.fr).

H. Bazzi is with Department of Electrical and Electronics Engineering, Lebanese International University, Beirut, Lebanon and A. Harb is with Department of Electrical and Electronics Engineering, The International University of Beirut, Beirut, Lebanon (e-mail: adnan.harb@liu.edu.lb).

II. OxRAM Technology

A. 1T1R memory cell

Devices used in our TRNG circuit are bipolar OxRAMs. An OxRAM consists of two metallic electrodes that sandwich a thin dielectric layer serving as a storage medium. This Metal-Insulator-Metal (MIM) structure, denoted RRAM in Fig. 1(a) can easily be integrated in the Back-End-Of-Line (BEOL) in combination with advanced CMOS technologies. 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 to form a capacitor-like structure [24, 25]. Fig. 1(b) shows the basic 1T1R memory cell. In this configuration one MOS transistor is serially connected to an OxRAM. This select transistor acts as a "local" 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 the FORMING and the SET operations. Table I presents the different voltage levels applied across the OxRAM cell presented in Fig. 1(b) during the different functioning phases. The whole experimental setup, based on a Keysight B1500 semiconductor parameter analyzer, will be described in section II.C. Fig. 2 presents typical 1T1R OxRAM I-V characteristics. Based on these I-V curves, the memory cell behavior can be seen as follows: after an initial electroforming step (not presented here for a better readability), 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 an HRS and an LRS. This resistance change is achieved by applying specific biases across the 1T1R cell (i.e. V_{SET}, switching from HRS to LRS and V_{RESET}, switching from LRS to HRS). According to Fig. 2, V_{SET} value required to switch from HRS to LRS is around 0.65 V, while V_{RESET} value required to switch back to HRS is around -0.65 V.

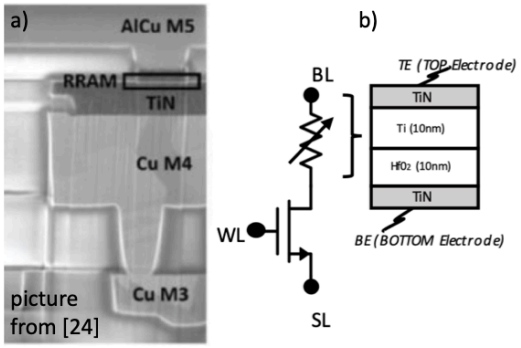

Fig. 1. (a) TEM cross-section of an OxRAM device co-integrated in a 130nm CMOS process (b) symbol view of a basic 1T1R OxRAM cell.

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	1.2V	0V	0V

The proposed TRNG circuit exploits the HfO_2-based OxRAM variability to generate a sequence of random bits. Indeed, HfO_2-based OxRAM technology suffers from stochastic switching and these statistical fluctuations are generally attributed to the formation/dissolution of a Conductive Filament (CF) between metallic electrodes [26-28]. 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 [29].

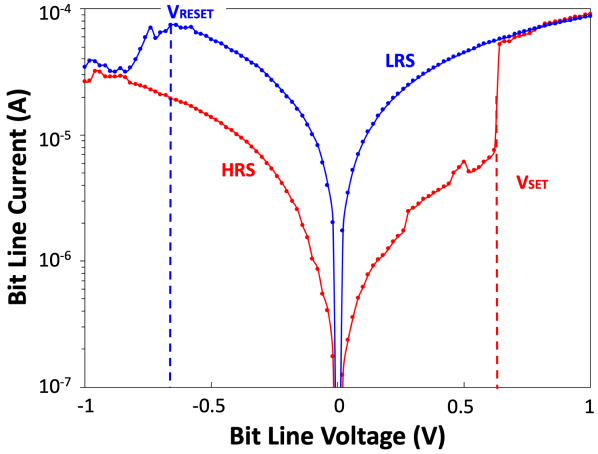

Fig. 2. I-V characteristics of an OxRAM cell, using the operating conditions from Table I. R_{SET} (blue) and R_{RESET} (red) levels are highlighted.

B. 1T1R memory array

Fig. 3(a) presents the used 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. 3(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).

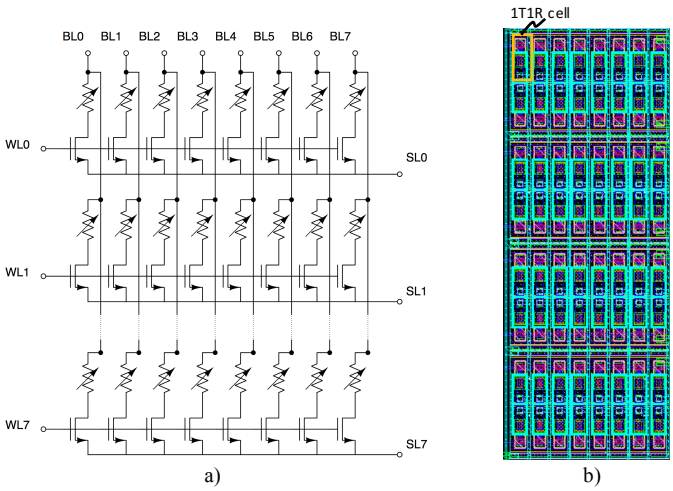

Fig. 3. (a) 8x8 OxRAM memory array and (b) corresponding layout view.

C. Experimental Setup

Fig. 4 describes the experimental setup which is based on a Keysight B1500 semiconductor parameter analyzer. The studied structure is the 7x7 1T1R OxRAM memory array presented in section II.B which is embedded on an 8-inch wafer, connected to the B1500 through a probe card and a low-resistance switching matrix. The matrix connects the Source/Measure Units (SMUs) to the memory array pads during the SET, RESET and READ operations. All the experiments are performed thanks to Python programs, controlling the equipment.

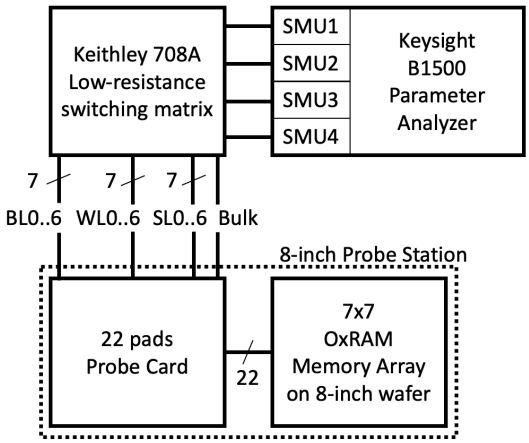

Fig. 4. Experimental setup used for the 7x7 OxRAM memory array.

D. 7x7 memory cell array experimental results

After an initial forming step (Table I) all the conductive filaments of the 49 memory cells are created and the 7x7 memory array is ready to use. Memory cells have first suffered 200 successive RESET/SET cycles to obtain the initial distribution of HRS resistances (after individual RESET operations) and LRS resistances (after individual SET operations). Fig. 5 presents these distributions and the inset shows resistance values for each cycle. Each distribution is made of 9,800 values (49x200). Fig 6. presents the corresponding HRS and LRS cumulative probabilities, using data from Fig. 5. It is worth noting that the HRS level is more spread than the LRS level which is a classical trend in OxRAM technology [25, 26]. The LRS median is around 12kΩ while the HRS median is around 150kΩ. We can notice on Fig. 5 and 6 an overlap between HRS and LRS distributions (i.e. some cells present an HRS resistance lower than some LRS resistance values). This is due to device to device variability combined with the programming conditions. This observation leads to the definition of the notion of "Resistance Threshold Level" referred to as R_{TH}.

If the resistance value is lower (resp. higher) than a threshold value denoted R_{TH}, the cell is considered in a Low Resistance Level LRL (resp. in High Resistance Level HRL), corresponding to a "1" (resp. "0") logical state. The choice of this threshold value R_{TH} for random number generation deserves a focus, it will be discussed in section III.B.

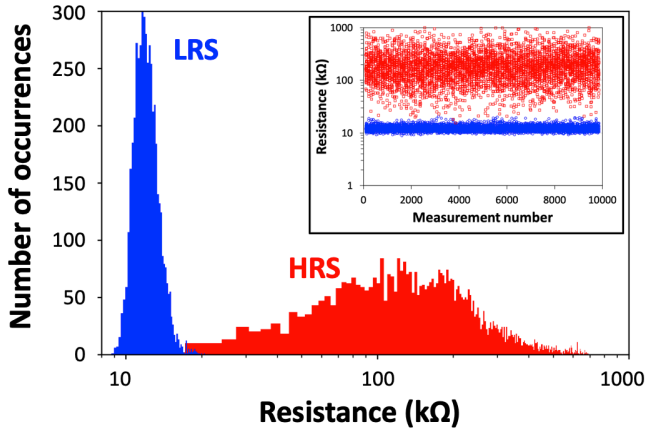

Fig. 5. Resistance values distribution after 200 consecutive individual SET/RESET cycles of the 7x7 array (9,800 LRS and 9,800 HRS values).

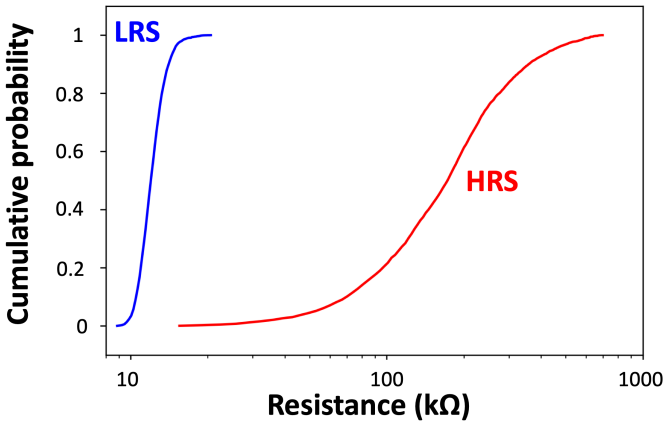

Fig. 6. Cumulative probabilities of the LRS and HRS resistances (using data from Fig. 5)

During a classical SET operation, the final cell resistance is a function of the maximal current allowed through the cell. This maximal current, flowing through the Bit Line, can be adjusted by modulating the Word Line bias V_{WL} connected to the gate of the memory cell select transistor (see Fig. 1(b) and Fig. 3(a)). Fig. 7 presents the impact of the Word Line voltage on the cell resistance value (left axis) during a SET operation. The impact on the maximal Bit Line current is also reported (right axis). In this figure, each Word Line voltage value is associated with 49 resistance values coming from every cell of the memory array. When the Word Line voltage is low the select transistor controls very well the current through the cell, while the current dispersion becomes larger when the Word Line voltage is high. The relation between the maximal current allowed in the memory cell and the current dispersion is presented in Fig. 8 and has already been observed in literature [16, 30]. We can observe that the higher the maximal current during a SET operation, the lower the resistance after SET. Moreover, when the maximal current decreases, the resistance values are more spread. Conversely, when the current limitation is high, all the cells are correctly SET switching in a low resistance state.

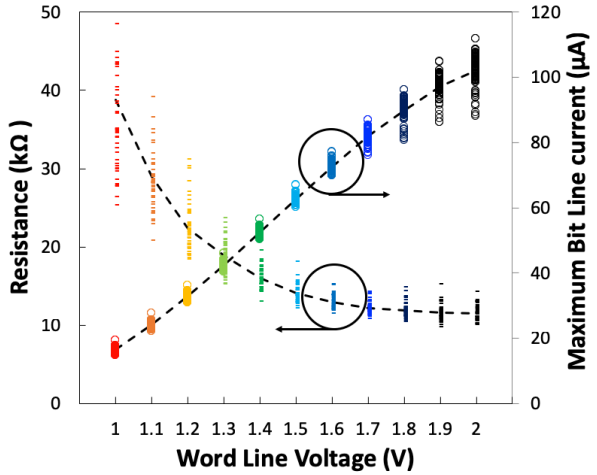

Fig. 7. Impact of the Word Line voltage on the final resistance and the maximum Bit Line current during individual cell SET operations for the 7x7 memory array.

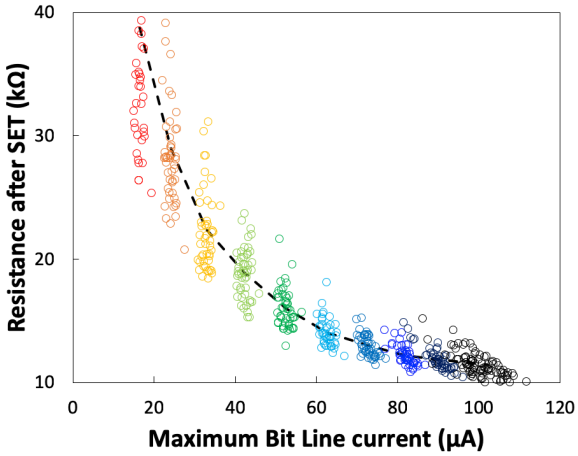

Fig. 8. Impact of the maximal cell current on the post-SET resistance for the 7x7 memory array (49 cells) where each cell is SET individually. Cell current limitation is achieved by controlling the select transistor gate bias.

III. TRNG Methodology

A. *TRNG concept: Input Current Limitation (ICL)*

The proposed TRNG concept is based on the following specific protocol referred to as the ICL technique for the random number generation: (i) OxRAM cells are first RESET one by one by addressing each cell independently, (ii) a global SET operation is performed with all BLs and WLs activated, with an Input Current Limitation I_{TOT} imposed by the B1500 generator and (iii) a READ operation is achieved to sense the cell resistance values. In a future circuit, a current source will be designed and integrated to the memory. Due to the current levels involved in this experiment (less than a few milliamps), the use of a single source for the whole array is possible. The most sensitive part is the global SET operation which results in a random distribution of the total input current I_{TOT} within the memory array (Fig. 9).

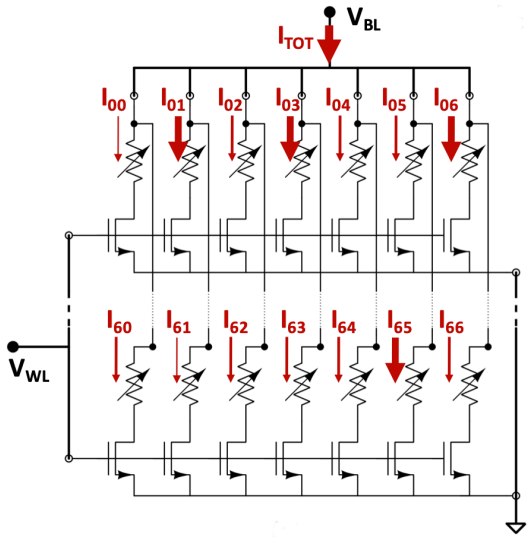

Fig. 9. Example of current distributions within the memory array using the Input Current Limitation (ICL) technique with a value of I_{TOT}. The thicker the arrow, the higher the current.

The random current distribution among the memory cells is due to the stochastic nature of OxRAM cells. Indeed, due to the variability, some "fast" cells can easily reach low resistance level (LRL), consuming a main part of the total current available so that the other cells cannot be SET anymore and remain in their high resistance level (HRL) or are slightly shifted to intermediate resistance values. Nevertheless, the current in a single cell is limited thanks to the WL voltage applied on the select transistor so that all the available current won't flow in this cell. Moreover, thanks to the cycle to cycle variability which is comparable to the device to device variability in this technology, the SET cells will not always be the same, avoiding reproducible spatial patterns to be created [8, 16, 17, 30-32]. Using data from Fig. 5 we show in Fig 10 that for the 49 cells in the array the Device-to-Device (for 100 cycles) and Cycle-to-Cycle (for 49 cells) variabilities are comparable. If this TRNG methodology is applied to another technology, a careful engineering of the applied pulses and electrical parameters (forming conditions, SET current limitation, …) is required to guarantee a Cycle-to-Cycle variability larger than the Device-to-Device one. In our study, the resistance of the interconnects has also been taken into account since we have demonstrated in a previous work the impact of voltage drop on this kind of memory array lines [33], that's why the memory array for the random number generation was limited to a 7x7 size.

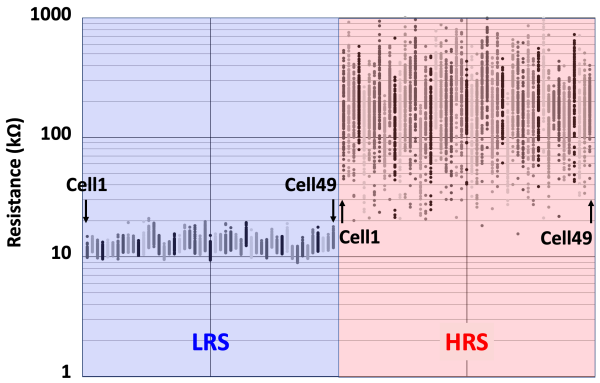

Fig. 10. Cycle-to-Cycle and Device-to-Device variabilities from data in Fig. 5.

B. *ICL implementation*

Fig. 11 illustrates the memory array current evolution versus the Bit Line Voltage V_{BL} for a single memory array (Fig. 9). As V_{BL} increases, memory cells are SET successively, inducing an increase of the memory array current. This is highlighted by the current steps of the red curve of Fig. 11, each step corresponding to the current contribution of individual cells of the array moving from an HRL level to an LRL level. When the array current reaches its maximal value I_{TOT}, a subset of the memory array cells is effectively in an LRL level while the rest of the array remained in an HRL level. Note that the total number of LRL cells is function of the maximal current value I_{TOT} (the higher I_{TOT}, the higher the number of LRL cells).

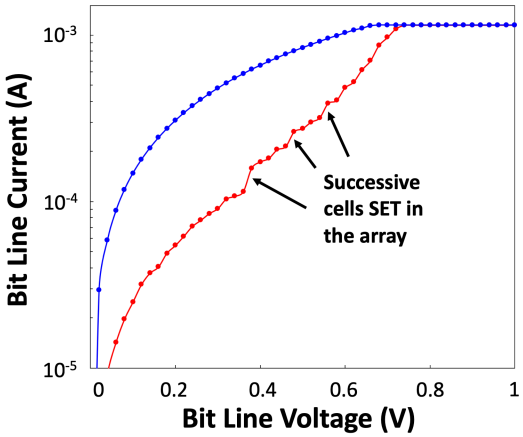

Fig. 11. I-V characteristics of the 7x7 OxRAM array, using the ICL technique during a global SET operation (I_{TOT} is here limited to 1150 µA).

C. *Choice of the threshold resistance R_{TH}*

Fig. 12 presents the ratio of LRL cells in the array versus the total current I_{TOT} for different threshold resistance values R_{TH} ranging from 15kΩ to 100kΩ (R_{TH} being defined as the resistance value below which a cell is in an LRL level).

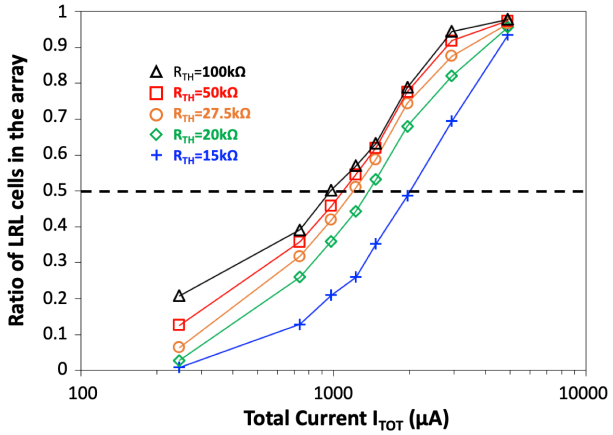

Fig. 12. Mean ratio (over 1,000 runs for each I_{TOT} using ICL technique) of LRL cells in the array.

Each point of Fig. 12 curves represents the HRL over LRL ratio obtain after 1,000 runs applied to the 7x7 array under the ICL technique for a fixed I_{TOT} value. The ICL method is repeated for different I_{TOT} values ranging from 200 µA to 5 mA. On the one hand, when the I_{TOT} current is very low (a few hundreds of micro-amps) only few cells can reach the LRL level since the current provided to the array is immediately consumed by some "fast" cells. Indeed, as shown in Fig. 11, "fast" cells have a lower SET voltage V_{SET} and are the first cells to conduct current as the BL voltage increases, thus all the other cells do not have enough current to reach a low resistance value after the SET operation as depicted in Fig. 8. On the other hand, when the current is high enough (few thousands of micro-amps), all the cells in the array can reach the LRL level since the current is self-limited in each cell by the select transistor. For a given I_{TOT}, when R_{TH} decreases, the number of cells is LRL level decreases. Thus, the choice of the threshold value R_{TH} is of crucial importance in the ICL implementation. Indeed, for TRNG applications and especially for NIST test suite success [34], 50% of the cells must statistically be in the LRL level so if we consider this 50% target (dashed line in Fig. 12) we can plot in Fig. 13 the total current I_{TOT} required for each R_{TH} values to obtain a 50% of LRL over HRL ratio, denoted $I_{TOT_{0.5}}$.

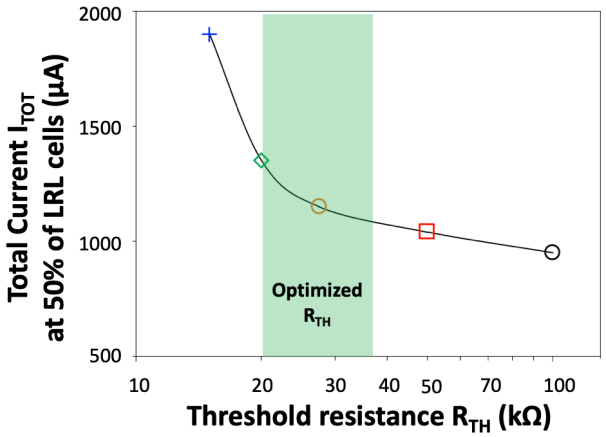

Fig. 13 Required I_{TOT} value to obtain 50% of LRL cells in the array as a function of the threshold resistance R_{TH}. Symbols for the different R_{TH} values are the same as in Fig. 12.

To reduce the current consumption of the proposed TRNG solution, we can see that the R_{TH} value cannot be too low since the required current is high. Consequently, the chosen R_{TH} should be higher than 20 kΩ. Moreover, if R_{TH} is too high, the LRL is directly included in the natural HRS distribution of the memory cell array (Fig. 5 and 6). Cells could stay in the LRL level, losing the required randomness feature, and compromising the NIST test suite success. Consequently, the chosen R_{TH} should be lower than 35 kΩ and included in the green area of Fig. 13. In the rest of the paper the R_{TH} value is equal to 27.5 kΩ. The associated current limitation I_{TOT} is equal to 1150 µA in order to SET exactly half of the memory array. Despite external (temperature, …) or internal variations (degradation, …) the 50% ratio of LRL cells has to be ensured. Concerning the degradation of our devices, it is possible to reach an outstanding endurance of twenty billion cycles on the technology considered in our paper, as shown in [35]. Nevertheless, the R_{TH} value (or equivalently the I_{TOT} value) has to be tuned for each random number generation step. Methods have been proposed in literature and can be adapted in our technology [4, 36, 37], based on a current comparator we proposed in a previous work [38]. We will discuss in section IV.E the robustness of our methodology and the real need to track the right R_{TH} value during the lifetime of the TRNG circuit.

D. *Modeling of the ratio of LRL cells in an array*

To interpolate the ratio r_{LRL} of LRL cells in an array of size N_{cell} (N_{cell} = 49 in our study), we propose a model using a generalized sigmoid function, according to the equation (1):

$$r_{LRL}(I_{TOT}) = \frac{N_{LRL}(I_{TOT})}{N_{cell}} = \frac{2}{1+e^{-C.(I_{TOT}-I_0)}} - 1 \quad (1)$$

where C and I_0 are two fitting constants.

The value of I_0 corresponds to the minimum current necessary to have a non-zero probability to have a cell in a LRL level.
I_0 can thus be estimated thanks to the values of V_{SET} (around 0.65 V) and R_{TH} using equation (2):

$$I_0 = \frac{V_{SET}}{R_{TH}} \approx \frac{0.65}{R_{TH}} \quad (2)$$

Consequently, the value of C can be calculated so that we obtain half of LRL cells in the array for a given value of I_{TOT}. By solving eq. (1) with $r_{LRL}(I_{TOT_{0.5}}) = \frac{1}{2}$ we can demonstrate (equation (3)) that:

$$C = \frac{\ln(3)}{I_{TOT_{0.5}} - I_0} \quad (3)$$

Fig. 14 shows that the fitting curves (dashed lines) obtained with this model are consistent with the experimental results.

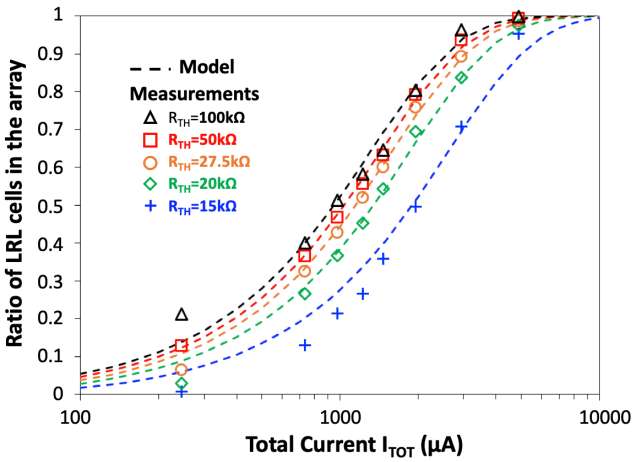

Fig. 14. Fitting curves of the proposed model for the mean LRL ratio (over 1,000 runs for each I_{TOT} using the ICL technique).

IV. NIST Results

A. *Analog bitmaps*

Between two consecutive runs, memory cells carry different current intensities, resulting in different final cell resistances. These results are confirmed by the bitmaps presented in Fig. 15. Bitmaps are extracted after two consecutive runs (N and N+1) and plotted as a 2D matrix. Resistance values are represented by a grayscale from white to black. Black is associated to the highest resistance values (higher than 440 kΩ) and white is associated to the lowest resistance values (lower than 13.75 kΩ).

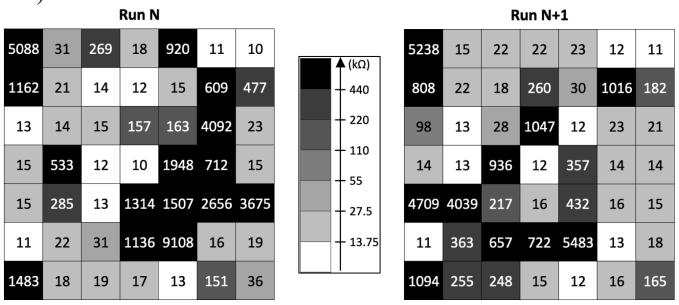

Fig. 15. Analog bitmaps after Run N (left) and Run N+1 (right) with resistance values (in kΩ) ranging from values lower than 13.75 kΩ (white) to values higher than 440 kΩ (black).

For the NIST test, we need to convert the analog values obtained from the 1,000 consecutive runs applied to a 49-cell array into 49,000 digital values.

B. *Digital bitmaps*

Fig. 16 presents the resistance distribution of the previous 49,000 analog values. The used color gradient is identical to the one used in Fig. 15.

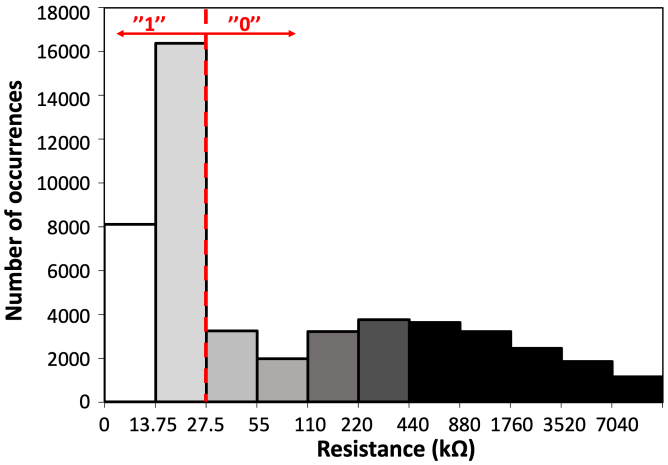

Fig. 16. Resistance distribution of 1,000 runs involving the 49 cells (49,000 occurrences) for I_{TOT} = 1150 µA using ICL technique. The greyscale values correspond to the ones from Fig. 15.

To convert resistance values into "0" and "1", all values lower than R_{TH} = 27.5 kΩ (dashed line of Fig. 16) 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. Thus, the analog bitmaps presented in Fig. 15 are turned into logical bitmaps presented in Fig. 17. At run N we obtain 25 bits at "1" level (and thus 24 bits at "0" level) and at run N+1 we obtain 26 bits at "1" level (and thus 23 bits at "0" level). Moreover, between the two presented runs 21 cells out of the 49 have changed their state and no systematic pattern is visible between the two runs. Over the 1,000 runs we performed; we have reached 49.96% of "1" bits which is very close to the 50% target.

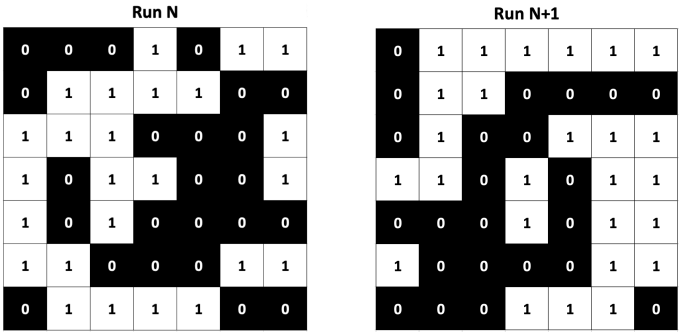

Fig. 17. Digital bitmaps after Run N (left) and Run N+1 (right) using data from Fig 15.

C. NIST results on 7x7 array

The random numbers (49 kbits) generated after 1000 runs and extracted from the distribution presented in Fig. 16 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 [34]. Without any post-processing stage, 6 NIST tests (over 15) were successful. Table II sums up the results of all the tests.

TABLE II. NIST TEST SUITE RESULTS ON 7X7 MEMORY ARRAY

Test	p-value	Random ?
[01]-Frequency	0.9909	**Yes**
[02]-Frequency within a block	1.0	**Yes**
[03]-Runs	2.6e-39	No
[04]-Longest Run of ones in a block	1.2e-68	No
[05]-Binary Matrix Rank	0.7062	**Yes**
[06]-Discrete Fourier Transform	0.0	No
[07]-Non-overlapping Template Matching	9.4e-104	No
[08]-Overlapping Template Matching	2.7e-71	No
[09]-Maurer's Universal Statistical	2.1e-27	No
[10]-Linear Complexity	0.5289	**Yes**
[11]-Serial	0.0	No
[12]-Approximate Entropy	0.0	No
[13]-Cumulative Sums	8.6e-8	No
[14]-Random Excursions	0.9977	**Yes**
[15]-Random Excursions Variant	0.8694	**Yes**
Global NIST Score		**6 / 15**

D. NIST results after XOR operation

To improve the entropy of the random bit stream, a post-processing step, based on a XOR gate is added as already proposed in previous studies found in the literature [20-23]. We propose to add, either directly inserted in the circuit or during a post-processing phase of the data, a XOR operation having as inputs the 49 bits of the array. The detailed implementation of cascaded-XOR gates is illustrated in Fig.18. Only 8 XOR gates and 7 D-Flip Flops are used. TRNG outputs are read by senses amplifiers connected to the memory array bit lines (OUT0 to OUT6). OUT0 to OUT6 are then XORed (4 gates) and sent to a 7-bit shift register (D-Flip Flops). When the shift process is over (S signal goes High), the shift register outputs are XORed again to provide the random bit.

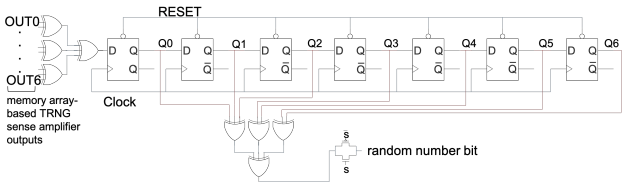

Fig. 18. Circuit performing the XOR operation between bits of the memory array.

If we consider the proposed TRNG circuit with an 7x7 elementary array, the area of the XOR circuitry is comparable to the one of the memory array as shown in table III.

TABLE III. SIMULTED AREAS OF XOR POST-PROCESSING

Gates	Area (µm2)
2-input XOR (x4)	43.04
3-input XOR (x7)	72.62
D flip-flop (x7)	118.4
Transmission gate (x1)	5
Total XORing Area	**$1.297x10^3$**
7x7 Memory array	**$1.2x10^3$**

Regarding the power consumption, power overhead associated with one random bit generation has been simulated as 41.5 µW with an average current of 20.7 µA. This current is negligible (less than 2%) compared to the current limitation I_{TOT} used to program the memory array which is equal to 1150µA. Table IV sums up the results of all the tests after a XOR-49 post-processing step: 12 over 15 NIST tests are successful. The only failed tests ([05]-Binary Matrix Rank, [08]-Overlapping Template Matching, [09]-Maurer's Universal Statistical) need a longer sequence of bits as recommended in [34]. Due to the experimental setup used for this study, data generation is quite slow (about one week for the 1,000 ICL runs). However, the proposed TRNG circuit is intended to be embedded in a dedicated circuit for a faster random data generation. Indeed, ReRAM and especially HfOx OxRAM have already been demonstrated to be very fast technologies [39, 40].

TABLE IV. NIST TEST SUITE RESULTS AFTER XOR-49 OPERATION

Test	p-value	Random ?
[01]-Frequency	0.6580	**Yes**
[02]-Frequency within a block	0.6752	**Yes**
[03]-Runs	0.9951	**Yes**
[04]-Longest Run of ones in a block	0.8351	**Yes**
[05]-Binary Matrix Rank	-1.0	No
[06]-Discrete Fourier Transform	0.7717	**Yes**
[07]-Non-overlapping Template Matching	0.6058	**Yes**
[08]-Overlapping Template Matching	-1.0	No
[09]-Maurer's Universal Statistical	-1.0	No
[10]-Linear Complexity	0.3208	**Yes**
[11]-Serial	0.9000	**Yes**
[12]-Approximate Entropy	0.9992	**Yes**
[13]-Cumulative Sums	0.7947	**Yes**
[14]-Random Excursions	0.9679	**Yes**
[15]-Random Excursions Variant	0.4308	**Yes**
Global NIST Score		**12 / 15**

E. Robustness of the proposed TRNG circuit

If for any reason (degradation, environmental change, etc.) a spatial pattern appears, the XOR operation will maintain the randomness of the generated number. Indeed, we have forced in the 49,000-bit sequence the 24 first cells at a stuck-ON '1' (or stuck-OFF '0') state during the 1,000 runs. After the XOR operation NIST tests still succeed with 12 pass tests over 15 NIST tests as previously presented in Table IV. The XOR step guarantees the robustness of the TRNG against spatial patterns (even if it is initially not supposed to happen due to the Cycle-to-Cycle and Device-to-Device variabilities presented in section III.A). On the other hand, the choice of R_{TH} seems to be crucial for proper operation of the proposed TRNG. Nevertheless, even if the original choice of R_{TH} is a major concern to initially ensure the 50% of '1', we have demonstrated that the final XOR operation guarantees the success of 12 over 15 NIST tests for a digitization with R_{TH} values ranging from 12kΩ to 43kΩ. This result establishes that during the circuit lifetime, parameters degradation will not affect the randomness of the generated bits as R_{TH} can vary to a certain extent, avoiding the need of a continuous operation of the probability tracking. This work is summarized and compared to the state-of-art of recent TRNGs in Table V.

TABLE V. COMPARISON TO STATE-OF-ART TRNGS

	Circuit Type	Techno. (nm)	Entropy Source	NIST pass	Power Eff. (pJ/bit)
This Work	**8x8 memory array**	**130**	**ReRAM switching current**	**12**	**138***
Ref [9] 2019	1Kb ReRAM array	N.A.	ReRAM cycle-to-cycle variability	All	3.5
Ref [20] 2017	Single cell	No CMOS**	ReRAM switching delay	15	N.A.
Ref [10] 2016	2 cells	N.A.	ReRAM switching delay	11	N.A.
Ref [11] 2016	Array***	40	ReRAM current fluctuation	All	40
Ref [12] 2015	CMOS	350	Thermal noise	7	120
Ref [19] 2012	Single cell	65	ReRAM RTN	5	N.A.

* during global SET with V_{BL}=1.2V, I_{TOT}=1150µA, t_{SET}=100ns
** Standalone ReRAM, not embedded in a CMOS technology
*** Array size not specified

V. CONCLUSION

The proposed TRNG is implemented based on an elementary array of 1T1R OxRAM cells. During a global SET operation, where all the array cells are selected, the programming current is limited (i.e. Input Current Limitation technique or ICL) with I_{TOT} = 1150 µA. As the available current is not enough to SET the whole memory array, the proposed programming technique results in a stochastic distribution of resistance values, due to the intrinsic variability of the cells. To convert resistance values into "0" and "1", a threshold resistance R_{TH} equals to 27.5 kΩ is chosen. The R_{TH} choice is crucial as it controls the circuit power consumption. Finally, the digital bit stream is confronted to NIST standard benchmarks. The bit stream passes 12 NIST tests, after a XOR post-processing step, which also increases the robustness of the proposed circuit against parameter degradation.

ACKNOWLEDGMENT

The authors wish to acknowledge the support from the CEA-Leti ("Commissariat à l'énergie atomique-Laboratoire d'électronique et de technologie de l'information"). CEA-Leti provided the technology access as part of the Memory Advanced Demonstrators project (MAD200).

REFERENCES

[1] V. Van der Leest, R. Maes, G. J. Schrigen, and P. Tuyls, "Hardware intrinsic security to protect value in the mobile market," *Highlights of ISSE 2014 Conf. Securing Electronic Business Processes*, 2014, pp 188-198. DOI: 10.1007/978-3-658-06708-3_15

[2] B. Gassend, D. Clarke, M. Van Dijk, and S. Devadas, "Silicon physical random functions," in *Proc. CCS '02*, Washington, DC, USA, 2002, pp. 148-160. DOI: 10.1145/586110.586132

[3] 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 *ISSCC Tech. Dig.*, San Francisco, CA, USA, 2006, pp. 1666-1675. DOI: 10.1109/ISSCC.2006.1696222

[4] W. H. Choi, Y. Lv, J. Kim, A. Deshpande, G. Kang, J.-P. Wang, and C. H. Kim, "A magnetic tunnel junction based true random number generator with conditional perturb and real-time output probability tracking," in *Proc. IEDM*, San Francisco, CA, USA, 2014, pp. 12.5.1-12.5.4. DOI: 10.1109/IEDM.2014.7047039

[5] S. Gaba, P. Sheridan, J. Zhou, S. Choi, and W. Lu, "Stochastic memristive devices for computing and neuromorphic applications," *Nanoscale*, vol. 5, no. 13, pp. 5872-5878, 2013. DOI: 10.1039/C3NR01176C

[6] Y. Wang, W. Wen, M. Hu, and H. Li, "A novel true random number generator design leveraging emerging memristor technology," in *Proc. GLSVLSI*, Pittsburgh, PA, USA, 2015, pp. 271-276. DOI: 10.1145/2742060.2742088

[7] S. Balatti, S. Ambrogio, Z. Wang, and D. Ielmini, "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. DOI: 10.1109/JETCAS.2015.2426492

[8] S. Yu, X. Guan, and H.-S. P. Wong, "On the stochastic nature of resistive switching in metal oxide RRAM: Physical modeling, Monte Carlo simulation, and experimental characterization," in *IEDM Tech. Dig.*, Washington, DC, USA, 2011, pp. 17.3.1-17.3.4. DOI: 10.1109/IEDM.2011.6131572

[9] B. Lin, Y. Pang, P. Yao, D. Wu, H. He, J. Tang, H. Qian, and H. Wu, "A High-speed and High-reliability TRNG based on analog RRAM for IoT security application," in *IEDM Tech. Dig.*, San Francisco, CA, USA, 2019, pp. 14.8.1-14.8.4. In Press

[10] 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," in *IEEE Transactions on Electron Devices*, vol. 63, no. 5, pp. 2029-2035, 2016. DOI: 10.1109/TED.2016.2537792

[11] Z. Wei, Y. Katoh, S. Ogasahara, Y. Yoshimoto, K. Kawai, Y. Ikeda, K. Eriguchi, K. Ohmori and S. Yoneda, "True Random Number Generator using current difference based on a fractional stochastic model in 40-nm embedded ReRAM," in *IEDM Tech. Dig.*, San Francisco, CA, USA, 2016, pp. 4.8.1-4.8.4. DOI: 10.1109/IEDM.2016.7838349

[12] Z. Chen, W. Yin and K. Boyle, "True Random Number Generator in 0.35um for RFID applications," in *Proc. EDSSC*, Singapore, 2015. DOI: 10.1109/EDSSC.2015.7285193

[13] A. Chen and M.-R. Lin, "Variability of resistive switching memories and its impact on crossbar array performance," in *Proc. IRPS*, Monterey, CA, USA, 2011, MY.7.1-MY.7.4. DOI: 10.1109/IRPS.2011.5784590

[14] S. Yu, X. Guan, and H.-S. P. Wong, "On the Switching Parameter Variation of Metal Oxide RRAM—Part II: Model Corroboration and Device Design Strategy," in *IEEE Trans. Electron Devices*, vol. 59, no. 4, pp. 1183-1188, Apr. 2012. DOI: 10.1109/TED.2012.2184544

[15] S. Sahay and M. Suri, "Recent trend in hardware security exploiting hybrid CMOS-resistive memory circuits" in Semiconductor Science and Technology, vol. 32, no. 12, pp. 123001. DOI: 10.1088/1361-6641/aa8f07

[16] A. Fantini, L. Goux, R. Degraeve, D.J. Wouters, N. Raghavan, G. Kar, A. Belmonte, Y.-Y. Chen, B. Govoreanu, M. Jurczak, "Intrinsic switching variability in HfO_2 RRAM," in *Proc. IMW*, Monterey, CA, 2013, pp. 30-33. DOI: 10.1109/IMW.2013.6582090

[17] D. Garbin, Q. Rafhay, E. Vianello, S. Jeannot, P. Candelier, B. De Salvo, G. Ghibaudo, L. Perniola, "Modeling of OxRAM variability from low to high resistance state using a stochastic trap assisted tunneling-based resistor network", in *Eurosoi ULIS*, pp.125-128, 26-28 Jan. 2015. DOI: 10.1109/ULIS.2015.7063789

[18] S. Sahay, A. Kumar, V. Parmar and M. Suri, "OxRAM RNG Circuits Exploiting Multiple Undesirable Nanoscale Phenomena," in *IEEE Transactions on Nanotechnology*, vol. 16, no. 4, pp. 560-566, July 2017. DOI: 10.1109/TNANO.2016.2647623

[19] 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," in *IEEE Elec. Dev. Lett.*, vol. 33, no. 8, pp. 608-612, June 2012. DOI: 10.1109/LED.2012.2199734

[20] H. Jiang, D. Belkin, S. E. Savel'ev, S. Lin, Z. Wang, Y. Li, S. Joshi, R. Midya, M. Rao, M. Barnell, Q. Wu, J. J. Yang, and Q. Xia, "A novel true random number generator based on a stochastic diffusive memristor," *Nature communications*, vol. 8, p. 882, Oct. 2017. DOI: 10.1038/s41467-017-00869-x

[21] E. I. Vatajelu, G. Di Natale, "High-Entropy STT-MTJ-Based TRNG", *IEEE Transactions on VLSI*, vol. 27, issue 2, pp. 491-495, 2019; DOI: 10.1109/TVLSI.2018.2879439

[22] N. Jiteurtragool, C. Wannaboon, T. Masayoshi, "True Random Number Generator based on compact chaotic oscillator", in *Proc. ISCIT*, Nara, Japan, 2015. DOI: 10.1109/ISCIT.2015.7458370

[23] E. Böhl, "Simple true random number generator for any semi-conductor technology", in IET Comput. Digit. Tech., vol. 8, issue 6, pp. 239-245, 2014. DOI: 10.1049/iet-cdt.2014.0029

[24] G. Molas, G. Sassine, C. Nail, D. A. Robayo, J.-F. Nodin, C. Cagli, J. Coignus, P. Blaise, and E. Nowak, "Resistive Memories (RRAM) Variability: Challenges and Solutions," *ECS Transactions*, vol. 86, no. 3, pp. 35-47, 2018. DOI: 10.1149/08603.0035ecst

[25] A. Grossi, E. Vianello, C. Zambelli, P. Royer, J.-P. Noel, B. Giraud, L. Perniola, P. Olivo, and E. Nowak, "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. DOI: 10.1109/TVLSI.2018.2805470

[26] S. Larentis, F. Nardi, S. Balatti, D. Gilmer, D. Ielmini, "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. DOI: 10.1109/TED.2012.2202320

[27] 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. DOI: 10.1109/TNANO.2015.2455235

[28] L. Larcher, A. Padovani, O. Pirrotta, L. Vandelli, G. Bersuker, "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. DOI: 10.1109/IEDM.2012.6479077

[29] F. M. Puglisi, L. Larcher, A. Padovani, and P. Pavan, "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. DOI: 10.1109/JETCAS.2016.2547703

[30] S. Ambrogio, S. Balatti, A. Cubeta, A. Calderoni, N. Ramaswamy and D. Ielmini, "Statistical Fluctuations in HfOx resistive-switching memory: part I – Set/Reset variability", in *IEEE Transactions on Electron Devices*, vol. 31, no. 8, pp. 2912-2919, 2014. DOI: 10.1109/TED.2014.2330200

[31] D. Garbin, E. Vianello, O. Bichler, Q. Rafhay, C. Gamrat, G. Ghibaudo, B. De Salvo and L. Perniola, "HfO2-Based OxRAM Devices as Synapses for Convolutional Neural Networks", in *IEEE Trans. Electron Devices*, vol. 62, no. 8, pp. 2494-2501, August 2015. DOI: 10.1109/TED.2015.2440102.

[32] R. Degrave, A. Fantini, N. Raghavan, L. Goux, S. Clima, B. Goroveanu, A. Belmonte, D. Linten and M. Jurczak, "Causes and consequences of the stochastic aspect of filamentary RRAM", in *Microelectronic Engineering*, vol. 147, pp. 171–175, 2015. DOI: 10.1016/j.mee.2015.04.025.

[33] H. Aziza, P. Canet and J. Postel-Pellerin, "Impact of Line Resistance Combined with Device Variability on Resistive RAM Memories," in Adv. in Sc. Techn. and Eng. Syst. Journal, vol. 3, no. 1, pp 11-17, 2018. DOI: 10.25046/aj030102.

[34] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo, "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications," *Nat. Inst. Standards Technol.*, Gaithersburg, MD, USA, Pub. 800-22, 2001.

[35] M. Bocquet, T. Hirztlin, J.-O. Klein, E. Nowak, E. Vianello, J.-M. Portal and D. Querlioz, "In-Memory and Error-Immune Differential RRAM Implementation of Binarized Deep Neural Networks," in *IEDM Tech. Dig.*, San Francisco USA, 2018, pp. 20.6.1-20.6.4. DOI: 10.1109/IEDM.8614639.

[36] W. Che, J. Plusquellic and S. Bhunia, "A non-volatile memory based physically unclonable function without helper data", in *Proc. of IEEE/ACM Int. Conf. Comput.-Aided Design (ICCAD)*, Nov. 2014, pp. 148–153. DOI: 10.1109/ICCAD.2014.7001345

[37] L. Zhang, Y. Cheng, W. Kang, L. Torres, Y. Zhang, A. Todri-Sanial and W. Zhao, "Addressing the Thermal Issues of STT-MRAM From Compact Modeling to Design Techniques", in *IEEE Transaction on Nanotechnology*, vol. 17, no. 2, march 2018. DOI: 10.1109/TNANO.2018.2803340

[38] H. Aziza, B. Majri, M. Mansour, A. Chehab and A. Perez, "A lightweight write-assist scheme for reduced RRAM variability and power", in

Microelectronics Reliability, vol. 88, pp.6-10, 2018. DOI: 10.1016/j.microrel.2018.07.065

[39] S. Menzel, M. Salinga, U. Böttger and M. Wimmer, "Physics of the switching kinetics in resistive memories," in *Advanced Functional Materials*, vol. 25, pp. 6306-6325, June 2015. DOI:10.1002/adfm.201500825.

[40] R. Fackenthal, M. Kitagawa, W. Otsuka, K. Prall, D. Mills, K. Tsutsui, J. Javanifard, K. Tedrow, T. Tsushima, Y. Shibahara and G. Hush, "A 16Gb ReRAM with 200MB/s write and 1GB/s read in 27nm technology," in *IEEE International Solid-State Circuits Conference Digest of Technical Papers (ISSCC)*, pp. 338-339, 2014. DOI: 10.1109/ISSCC.2014.6757460.