True random number generation exploiting SET voltage variability in resistive RAM memory arrays

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

True Random Number Generation Exploiting SET Voltage Variability in Resistive RAM Memory Arrays

Jeremy Postel-Pellerin[1], Hussein Bazzi[1&2], Hassen Aziza[1], Pierre Canet[1], Mathieu Moreau[1], Vincenzo Della Marca[1], Adnan Harb[3]

[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

jeremy.postel-pellerin@im2np.fr

***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, the voltage applied to the cells of the memory array is fixed at the median SET voltage of the distribution, 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, 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 eleven NIST tests out of fifteen without any post-processing.**

Keywords- 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, 8].

OxRAM devices intrinsically suffer from significant spatiotemporal variability [9, 10]. Switching parameters vary from device to device and cycle to cycle [11, 12]. 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 the SET voltage variability of an OxRAM memory array. We propose to limit the voltage during the SET operation to the median SET voltage obtained from the memory array SET voltage distribution. In these conditions, it is expected that half of the cells in the array will switch to Low Resistive State (LRS) while the other half will remain in a High Resistive State (HRS), resulting in a stochastic distribution of resistance values across the array. Afterward, resistance values are converted into logical values to generate a random bit stream. The proposed TRNG overcomes limitations of state of the art OxRAM-based TRNG which are mainly based on a single memory cell [6, 7, 13, 14]. 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.

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, experimental results are provided and National Institute of Standards and Technology (NIST) test results are given. Finally, section IV provides some concluding remarks.

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 [15, 16]. 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 SET operations.

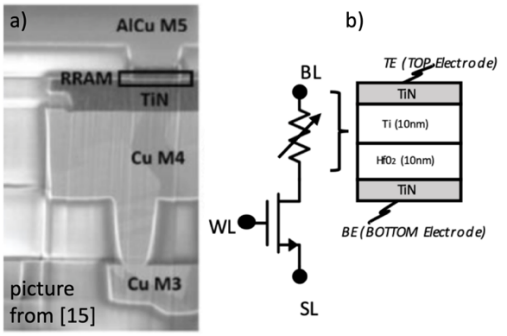

Fig. 1. (a) TEM cross-section of an OxRAM device co-integrated in a 130nm CMOS process (from [15]) (b) symbol view of a basic 1T1R OxRAM cell.

Table I presents the different voltage levels applied to the OxRAM cell presented in Fig. 1(b) during the different functioning phases. The whole experimental setup is based on a Keysight B1500 semiconductor parameter analyzer. The studied structure, presented in section II.B, 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.

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 [17-19]. 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 [20].

Fig. 2 presents typical 1T1R OxRAM I-V characteristics in linear scale, according to Table I programming conditions. 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). Fig. 2 also highlights the SET variability (V_{SET}). SET variability is here demonstrated after 7 consecutive RESET/SET operations.

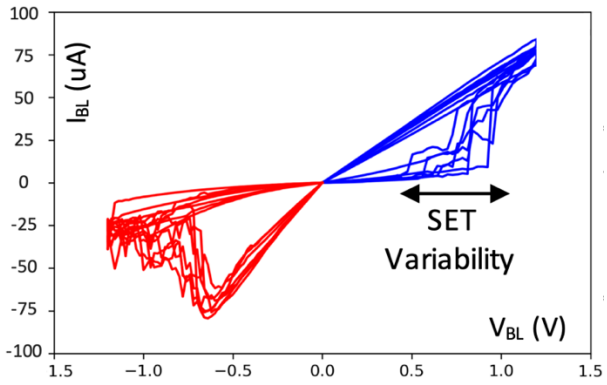

Fig. 2. I-V characteristics of an OxRAM cell, where V_{SET} variability is highlighted. Curves are obtained for 7 consecutive RESET/SET operations according to Table I programming conditions.

B. 1T1R memory array

Fig. 3(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. 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).

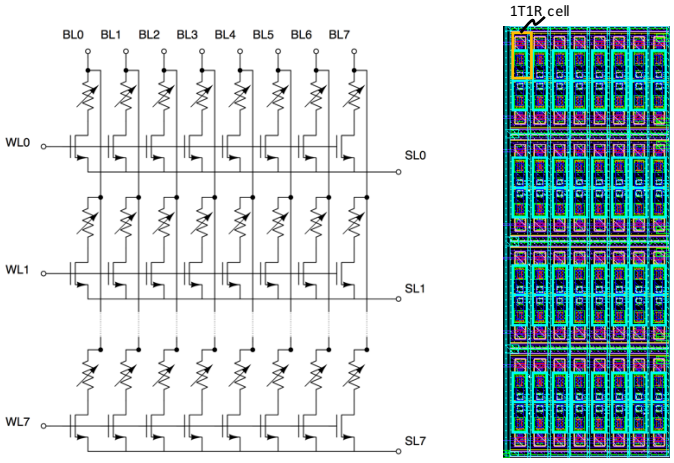

Fig. 3. (a) 8x8 OxRAM memory array and (b) corresponding layout view.

To extract the V_{SET} distribution, the memory array is first RESET. Then, memory cells are SET one by one to extract the V_{SET} threshold which is defined as the minimal voltage across the cell needed to reach 1µA. To catch Cycle to Cycle (C2C) as well as Device to Device (D2D) variability, the RESET/SET process is repeated 100 times for the whole array. Fig. 4 presents the resulting V_{SET} distribution.

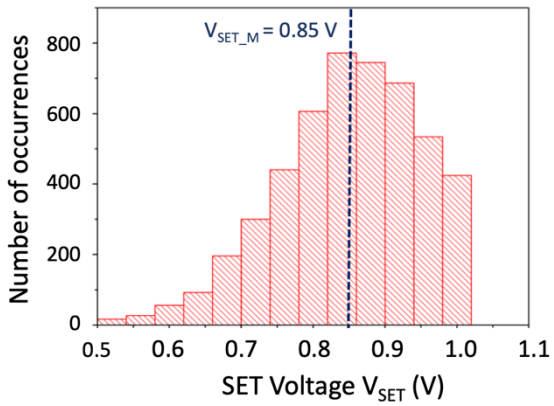

Fig. 4. SET Voltage (V_{SET}) distribution for 100 cycles on the memory array.

From distribution in Fig. 4, the median value V_{SET_M} is extracted and presented in Table II along with the distribution main parameters.

TABLE II. V_{SET} DISTRIBUTION PARAMETERS

σ	Min	**Median**	Max
0.098V	0.51 V	0.85 V	1.01 V

III. TRNG METHODOLOGY

From this point the TRN generation process consists in resetting the whole memory array and setting each cell individually with V_{SET_M} = 0.85V. As a result, some cells are switched in LRS state, while others remain in their initial HRS state, resulting in a random distribution of resistance values. Here again, the process is repeated 100 times. 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). The SET cells must not always be the same to avoid reproducible spatial patterns to be created. The resistance of the interconnects has thus been taken into account since we have demonstrated in a previous work the impact of voltage drop on this kind of memory array lines [21], that's why the memory array for the random number generation was limited to a 7x7 size.

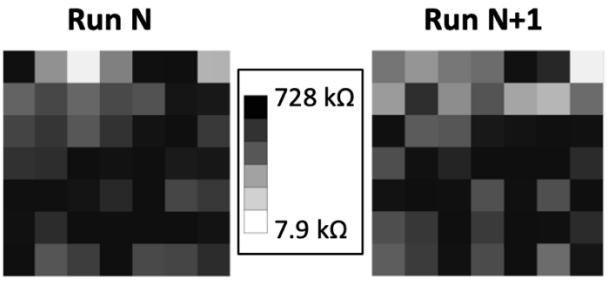

Fig. 5. Analog 2D bitmap after Run N (left) and Run N+1 (right) with resistance values ranging from 7.9 kΩ (white) to 728 kΩ (black)

Fig. 6 presents the resistance distribution which median value is equal to 145.5 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. 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 [22]. Nevertheless, the R_M value (or equivalently the V_{SET_M} value) can be tuned for each random number generation step. Methods have been proposed in literature and can be adapted in our technology [4, 23, 24], based on a current comparator we proposed in a previous work [25].

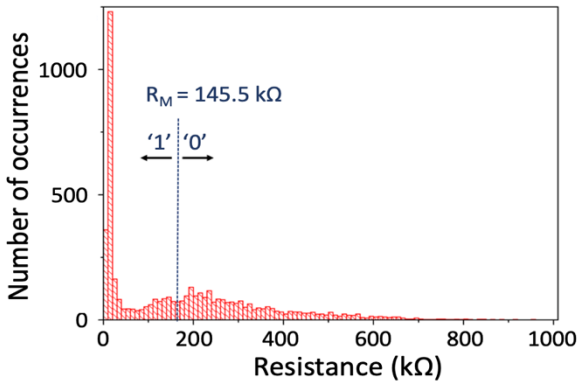

Fig. 6. Resistance distribution after 100 consecutive memory array RESET/SET operations

To convert resistance values into "0" and "1", all values lower than R_M = 145.5 kΩ (dashed line of 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. Thus, the analog bitmaps presented in Fig. 5 are turned into logical bitmaps presented in Fig. 7. At run N we obtain 24 bits at "1" level (and thus 25 bits at "0" level) and at run N+1 we obtain 25 bits at "1" level (and thus 24 bits at "0" level). Moreover, between the two presented runs 17 cells out of the 49 have changed their state and no systematic pattern is visible between the two runs.

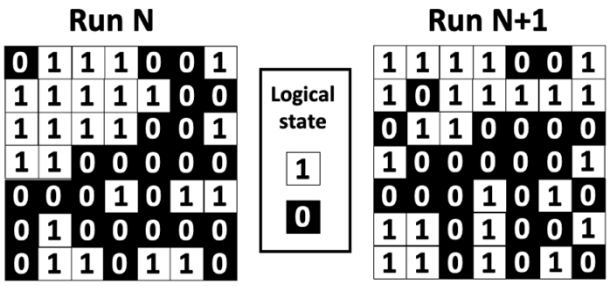

Fig. 7. Digital 2D bitmap after Run N (left) and Run N+1 (right) using data from Fig. 5

The random numbers (4.9 kbits) generated after 100 runs and extracted from the distribution presented in Fig. 6 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 [26]. The bitstream passes 11 NIST tests over 15 (see Table III) without any post-processing step. The only failed tests (05-Binary Matrix Rank, 08-Overlapping Template Matching, 09-Maurer's Universal Statistical, 10-Linear

Complexity) need a longer sequence of bits as recommended in [26]. Due to the experimental setup used for this study, data generation is quite slow (several hours for the 100 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 [27-29].

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

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**

IV. CONCLUSION

The proposed TRNG is implemented based on an elementary array of 1T1R OxRAM cells. Memory cells of an elementary array are first RESET one by one. Then, each cell is SET to extract the V_{SET} distribution of the array. The median value of the V_{SET} distribution is then used as the SET voltage for the next programming cycle. Based on this programming technique, it is possible to obtain random numbers presenting a perfect balance between '1' and '0'. These results have been confirmed after NIST tests. Indeed, the obtained bitstream passes 11 NIST tests over 15 without any post-processing step.

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] 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

[10] 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

[11] 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

[12] 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

[13] 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

[14] 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

[15] 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

[16] 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

[17] 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

[18] 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

[19] 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

[20] 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

[21] 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

[22] 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

[23] 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

[24] 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 Transactions on Nanotechnology*, vol. 17, no. 2, march 2018. DOI: 10.1109/TNANO.2018.2803340

[25] 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

[26] 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

[27] 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.

[28] 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

[29] E. I. Vatajelu, H. Aziza and C. Zambelli, "Nonvolatile memories: Present and future challenges," in *Proc. IDT '14*, Algiers, Algeria, 2014. DOI: 10.1109/IDT.2014.7038588