This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/LED.2018.2886396, IEEE Electron Device Letters

Unpredictable Bits Generation based on RRAM Parallel Configuration

Daniel Arumí, Álvaro Gómez-Pau, Salvador Manich, Rosa Rodríguez-Montañés, Mireia Bargalló González, and Francesca Campabadal

1

***Abstract*—In this letter a cell with the parallel combination of two TiN/Ti/HfO$_2$/W resistive random access memory (RRAM) devices is studied for the generation of unpredictable bits. Measurements confirm that a simultaneous parallel SET operation in which one of the two RRAMs switches to the low resistance state (LRS) is an unpredictable process showing random properties for different sets of cells. Furthermore, given a device pair, the same device switches during subsequent write operations. The proposed cell is also analyzed under different current compliances and pulse widths with the same persistent behavior being observed. The features of the proposed cell, which provide data obfuscation without compromising reliability, pave the way for its application in Physical Unclonable Functions (PUFs) for hardware security purposes.**

***Index Terms*— RRAM, variability, PUF, hardware security.**

I. Introduction

RRAMs (Resistive Random Access Memories) show intercell and cycle-to-cycle variability due to the stochastic nature of the switching mechanism, with the corresponding impact on their resistance [1]. This variability is one of the major limitations for the massive commercialization of these devices [2]. Nevertheless, the very same challenge has positioned RRAMs as one of the most promising candidates for the development of hardware security applications. In fact, recent works have explored the use of RRAMs in PUFs (Physical Unclonable Functions) [3]-[13]. A hardware PUF [14]-[15] is a security primitive that takes advantage of manufacturing variations to derive a secret from the physical characteristics of integrated circuits (ICs). PUFs are intended for device authentication and secret key storage purposes. Hence, they must produce uniformly distributed, independent and robust random bits. Most existing RRAMs PUFs are based on memory arrays with 1T1R (1 transistor – 1 resistor) cells or passive crossbars [3]-[13]. Regardless of the structure, a common approach to generating random bits (secret) consists in first inducing the same resistance state to every RRAM, and then performing the sensing procedure. This sensing procedure is based on comparing the RRAM resistance against a reference or performing a pairwise comparison [3], [5], [8]. This approach makes the extraction of the secret difficult for an attacker. However, effects such as retention loss, thermal dependence of the state or instability during the read process may cause bit-flipping during the comparisons, with the resulting impact on PUF reliability [16]. Some alternatives solve this limitation by setting half of the RRAMs in the high resistance state (HRS) and the other half in the low resistance state (LRS) [6]-[7], [10]-[11]. All these approaches may be potentially vulnerable since the secret is always unmasked.

The present letter investigates the behavior of a cell composed of two parallel RRAMs for the generation of unpredictable bits. In this work we call unpredictable bit a bit the value of which may be either 0 or 1 with equal probabilities and is determined by an unpredictable event. This event appears the first time the two RRAMs are brought in competition, after which it becomes repetitive. The idea of competing elements for the generation of unpredictable bits has also been proposed with AF gates [17]. The association of RRAMs has already been exploited for hardware security applications [18]-[21]. In fact, the work in [21] proposed a PUF implementation based on the parallel configuration of RRAMs, but it was analyzed only at simulation level. In this work, we experimentally demonstrate the behavior of the parallel association of RRAMs for the generation of unpredictable bits. The results, focused at cell level, confirm its potential application for PUFs.

II. Experimental set-up

The RRAM devices used in the experiments are TiN/Ti/HfO$_2$/W structures. The 10nm-thick HfO$_2$ layer was deposited by atomic layer deposition (ALD) at 225ºC using TDMAH and H$_2$O as precursors, and the top and bottom metal electrodes were deposited by magnetron sputtering. The bottom electrode consists of a 200nm-W layer and the top electrode of a 200nm-TiN and a 10nm-Ti layer acting as oxygen getter material. Fig. 1(a) shows a schematic cross-section of the final device structure. Fig. 1(b) is a top view microscope image of the resulting structures, which are square cells of 60x60 μm^2, 15x15 μm^2 and 5x5 μm^2.

The electrical characterization of the devices was performed using two synchronized Keysight B2912A Precision Source/Measure Units (SMUs). The instruments were connected to a computer via GPIB and controlled using MATLAB in order to automatically perform successive measurements.

First, the resistive switching behavior of every device was assessed under DC conditions. Double-sweep voltage ramps were applied from 0 to +1.1 V for the SET operation and from 0 to -1.4 V for the RESET operation. Typical resistive-switching characteristics are shown in Fig. 2(a). Voltage pulses were then programmed and applied in order to evaluate the resistive switching behavior in the pulse mode. The same voltage amplitudes as those in DC conditions were used for the

D. Arumi, A. Gómez-Pau, S. Manich and R. Rodríguez-Montañés are with the Departament d'Enginyeria Electrònica, Universitat Politècnica de Catalunya, Barcelona, 08028, Spain (e-mail: daniel.arumi@upc.edu, alvaro.gomez-pau@upc.edu, salvador.manich@upc.edu, rosa.rodriguez@upc.edu).

M. B. González and F. Campabadal are with the Institut de Microelectrònica de Barcelona-Centre Nacional de Microelectrònica, Consejo Superior de Investigaciones Científicas. Bellaterra 08193, Spain (e-mail: mireia.bargallo.gonzalez@csic.es; francesca.campabadal@imb-cnm.csic.es).

switching operations. The corresponding cycling behavior under pulse mode for a single device is shown in Fig 2(b).

Once the proper independent operation of two RRAMs was validated, the experiments with the proposed cell were performed. Its configuration is depicted in Fig. 3(a), where two RRAMs (R_1 and R_2) are connected in parallel. The common bottom electrode (V_G) is connected to a grounded resistor (R_G). The voltage pulse sequences were applied to the top electrodes of R_1 and R_2, as indicated in Fig. 3(b). Note that the SET and RESET operations were applied simultaneously to both devices and V_G is grounded during the RESET operation. No current compliance (I_{COMP}) was applied during the pulse sequences.

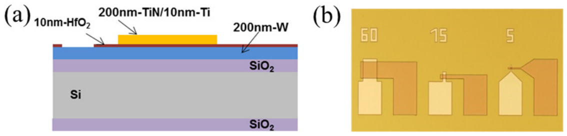

Fig. 1: (a) Schematic device cross-section (b) Top view optical microscope image.

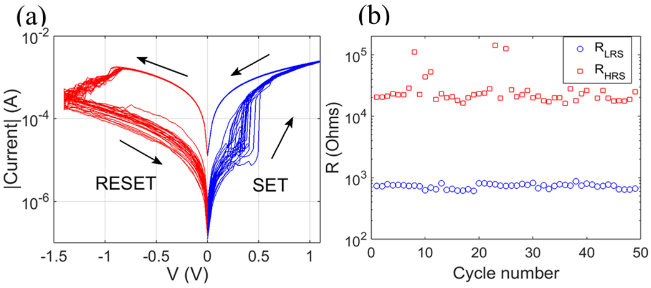

Fig. 2: (a) DC Resistive switching behavior during successive SET and RESET operations (b) R_{HRS} and R_{LRS} resistances during pulsed SET and RESET operations for a single RRAM.

III. Results and Discussion

The experimental results for a single parallel RRAM cell after 150 pulse sequences are shown in Fig. 4. The equivalent cell resistances are plotted after every RESET (Fig. 4(a)) and SET (Fig. 4(b)), respectively. The behavior of the cell is as follows: with both devices initially in the HRS, after the SET operation, one of the RRAMs switches to the LRS. When this device switches to the LRS, V_G increases preventing the other device from performing the switch. In the example in Fig. 4, R_2 is the switching device whereas R_1 always remains in the HRS. However, for a given cell, the RRAM that first switches to the LRS is unpredictable and this behavior can be exploited as the source of randomness. Furthermore, it is worth noting that during subsequent RESET operations, only the RRAM in the LRS switches, since the other one always remains in the HRS. This persistent behavior does not seem to depend on set voltage (V_{SET}). As an example of this, Fig. 5(a) shows the values of V_{SET} measured during the DC characterization for two RRAMs of a given cell. Despite the ranges of V_{SET} were overlapped, R_2 was always the switching device in the parallel configuration. The operation of the proposed cell is also independent of the set-up. Fig. 5(b) illustrates the results of the experiment with an RRAM pair where the pulse sequences were paused after 125 cycles. Connections were then exchanged, so that R_1 became R_2 and vice versa. Subsequently, the experiment was restarted. Observe how the switching device is always the same.

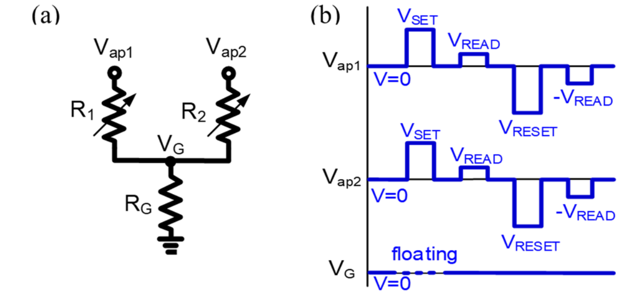

Fig. 3: Parallel RRAM cell (a) Schematic and (b) Diagram of voltage pulses with V_{SET} = 1.1 V, V_{RESET} = -1.4 V and V_{READ} = 0.1 V.

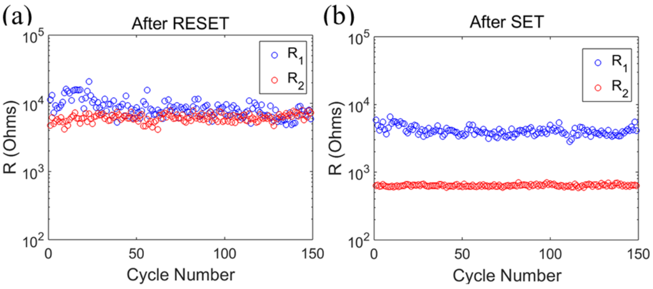

Fig. 4: Measured resistances of the RRAMs pair during cycling after parallel (a) RESET and (b) SET operations with R_G=500Ω. Systematic switching is found in a single cell.

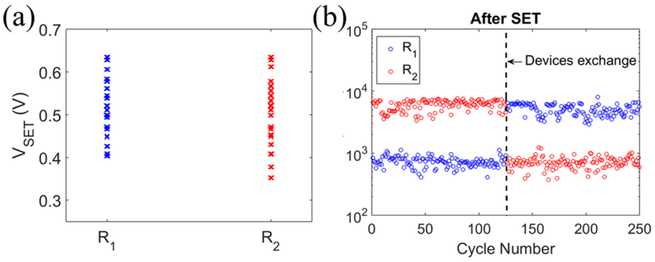

Fig. 5: (a) Set voltage V_{SET} obtained for 25 cycles during DC characterization for the RRAMs of the same cell. (b) Measured resistances of the RRAMs pair during cycling after parallel SET. R_1 and R_2 were exchanged in the middle of the experiment. Systematic switching for the same device is obtained.

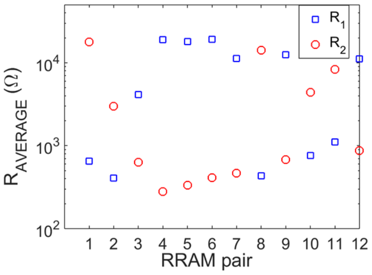

Fig. 6: Average resistance for R_1 and R_2 after a simultaneous SET operation for twelve parallel RRAMs cells, where 250 pulse sequences were considered for every cell. R_1 and R_2 resistances after a SET operation are different between cells and cannot be predicted.

Experiments were performed for a set of 35 RRAMs cells and the above behavior was confirmed. In fact, R_1 was the switching device for 16 out of 35 cells whereas R_2 was the switching device for the remaining 19 cells. For 12 of these cells, 250 pulse sequences were applied to each of them. A summary of the obtained results is given in Fig. 6. The reported average resistances for R_1 and R_2 after a simultaneous SET indicate that the systematic switching RRAM can be, indistinctly, either one of the two devices.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/LED.2018.2886396, IEEE Electron Device Letters

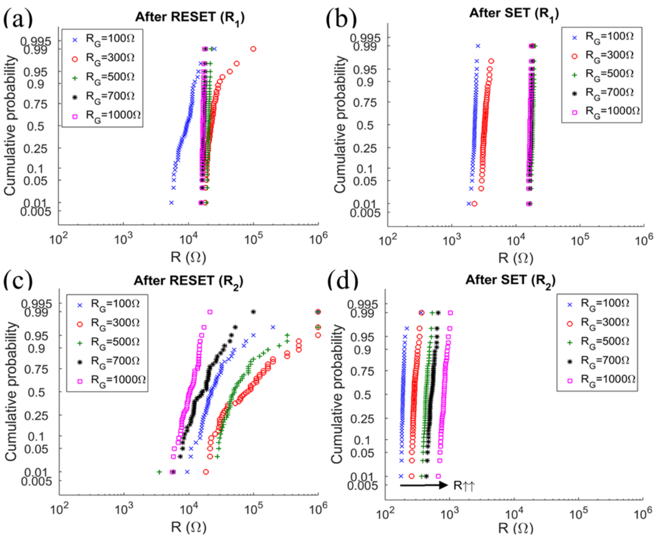

Fig. 7: Cumulative probability distributions for the resistances of a parallel RRAM cell for different R$_G$ values. A sequence of 50 cycles has been considered for every R$_G$ value (a) R$_1$ after RESET (b) R$_1$ after SET (c) R$_2$ after RESET and (d) R$_2$ after SET.

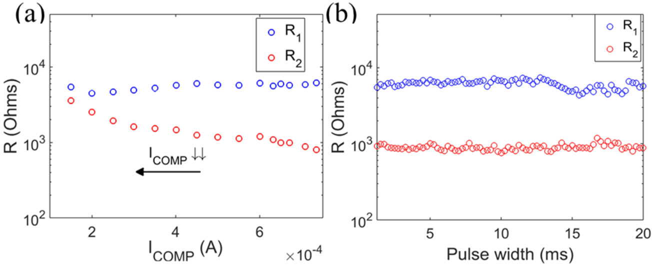

Fig. 8: Resistances of a parallel RRAMs cell after applying a SET operation (a) I$_{COMP}$ swept (b) Pulse width swept.

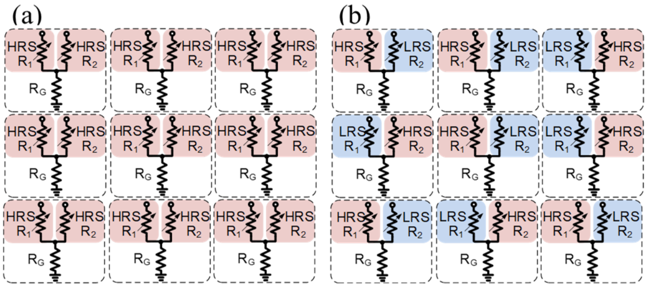

Fig. 9: Array of parallel RRAMs cells (a) Initially every device is in the HRS (b) Unpredictably, one of the two RRAMs of every cell switches to the LRS after a SET operation.

The switching properties of the proposed cell can be modified by adjusting the value of the serial resistor R$_G$ because it acts as a current limiter. In addition, its resistance must be appropriately selected to ensure the switching of only one of the two RRAMs. If R$_G$ is too low, the voltage across the non-switching RRAM will be high enough to undergo a (partial) switching to the LRS during the SET operation. This is shown in Fig. 7 where a cell behavior is reported using different R$_G$ values after every RESET (Fig. 7(a) and Fig. 7(c)) and SET (Fig. 7(b) and Fig. 7(d)). Note that, although the switching device is R$_2$, for low R$_G$ values (100 Ω and 300 Ω) R$_1$ also undergoes a partial switch to a low resistance state (Fig. 7(b)). However, this behavior is not observed at higher R$_G$ values.

The proposed cell was also analyzed under different I$_{COMP}$ and pulse widths. The results in Fig. 8(a) show that I$_{COMP}$ controls the resistance difference between both RRAMs after a SET operation, without affecting the switching behavior. During a parallel SET, as V$_G$ increases due to the switching of one of the RRAMs, the non-switching RRAM undergoes an intermediate voltage during the rest of the pulse. In this context, experiments where the pulse width was increased during the SET operation were conducted. The results are shown in Fig. 8(b) without influence of the pulse width in the range evaluated.

From these results, it is plausible to combine multiple cells in an array structure, obtaining a PUF-like implementation, as shown in Fig. 9(a). A single SET operation is initially required at every cell of the array to unmask the set of unpredictable bits (secret), see Fig. 9(b). No more write operations are required and only read operations need to be applied to sense the secret. The read process may consist in sensing the voltage at the common electrode when a read voltage is applied to the top electrode of either one of the RRAMs, with the top electrode of the other device grounded. Note that this voltage must be higher than the read voltage applied for a single RRAM. However, security may be compromised if an attacker tries to extract the secret while it is unmasked. This threat can be minimized if we take advantage of the persistent switching behavior during sequential operations. As soon as the secret stops being used, the cell can be obfuscated by applying a RESET operation, thus forcing both devices to the HRS. Hence, the measurement of the RRAMs resistances will not leak the stored bits, even if the circuit is powered off. In addition, subsequent SET operations will unmask the bits when needed. A PUF-like implementation based on the proposed cell is not expected to be susceptible to reliability issues caused by read instability, retention loss or thermal dependence, since the two RRAMs in a given cell are in different resistance states during the read-out. As in many PUF implementations, cells with unstable behavior may appear, inducing errors. This issue is addressed by incorporating error-correcting techniques or an allowable error threshold [15].

IV. Conclusion

For the first time, it was experimentally shown that two parallel RRAMs can be exploited as a basic cell for the generation of unpredictable bits. The simultaneous SET of two parallel RRAMs triggers a stochastic switch of one of the devices. The switching of one of the RRAMs between high and low resistance states persists during subsequent SET and RESET operations whereas the other RRAM always remains in a high resistance state. The observed behavior allows data obfuscation without compromising reliability. These features make this cell appealing for hardware security applications. In fact, the combination of multiple cells could be leveraged for potential implementation of a PUF-like structure.

Acknowledgment

This work has been partially supported by the Spanish Ministry of Science, Innovation and Universities, projects references TEC2013-41209-P, TEC2017-84321-C4-1-R and TEC2014-54906-JIN, with support of FEDER funds. This work has made use of the Spanish ICTS Network MICRONANOFABS.

REFERENCES

[1] S. Yu, X. Guan, H.-S P. Wong, “On the stochastic nature of resistive switching in metal oxide RRAM: Physical modeling, monte carlo simulation, and experimental characterization”, Proceedings of the IEEE International Electron Devices Meeting (IEDM) 2011, pp. 17.3.1 - 17.3.4, DOI: 10.1109/IEDM.2011.6131572.

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

[3] J. Rajendran, G.S. Rose, R. Karri, M. Potkonjak, “Nano-PPUF: A memristor-based security primitive”, Proceedings of the IEEE Computer Society Annual Symposium on VLSI 2012, pp. 84-87. DOI: 10.1109/ISVLSI.2012.40.

[4] L. Zhang, X. Fong, C.-H, Chang, Z.H. Kong, K. Roy, “Feasibility study of emerging non-volatile memory based physical unclonable functions” Proceedings of the IEEE 6th International Memory Workshop (IMW), 2014, pp.1-4, DOI: 10.1109/IMW.2014.6849384.

[5] J. Rajendran, R. Karri, J.B. Wendt, M. Potkonjak, N. McDonald, G.S. Rose, B. Wysocki, “Nano meets security: Exploring nanoelectronic devices for security applications”, Proc. IEEE 103 (2015) 829-849, DOI: 10.1109/JPROC.2014.2387353.

[6] A. Chen, “Utilizing the variability of resistive Random Access Memory to implement reconfigurable physical unclonable functions” IEEE Electron Device Lett. 36 (2015) 138-140, DOI: 10.1109/LED.2014.2385870.

[7] A. Chen, “Reconfigurable physical unclonable function based on probabilistic switching of RRAM”, Electron. Lett., 51 (2015) 615-617, DOI: 10.1049/el.2014.4375.

[8] R. Liu, H. Wu, Y. Pang, H. Qian, S. Yu, “Experimental characterization of physical unclonable function based on 1 kb Resistive Random Access Memory arrays”, IEEE Electron Device Lett. 36 (2015) 1380-1383, DOI: 10.1109/LED.2015.2496257.

[9] A. Mazady, M.T. Rahman, D. Forte, M. Anwar, “Memristor PUF—A Security Primitive: Theory and Experiment” IEEE IEEE J. Emerg. Sel. Top. Circuits Syst. 5 (2015) 222-229, DOI: 10.1109/JETCAS.2015.2435532.

[10] P.-Y Chen, R. Fang, R. Liu, C. Chakrabarti, Y. Cao, S. Yu, “Exploiting resistive cross-point array for compact design of physical unclonable function”, Proceedings of the IEEE International Symposium on Hardware Oriented Security and Trust (HOST) 2015, pp. 26-31, DOI: 10.1109/HST.2015.7140231.

[11] Y. Pang, H. Wu, B. Gao, N. Deng, R. Liu, S. Yu, A. Chen, H. Qian, “Optimization of RRAM-based physical unclonable function with a novel differential read-out method” IEEE Electron Device Lett. 38 (2017) 168-171, DOI: 10.1109/LED.2016.2647230,

[12] M. Uddin, M. B. Majumder and G. S. Rose, “Robustness Analysis of a Memristive Crossbar PUF Against Modeling Attacks”; IEEE Transactions on Nanotechnology, vol. 16, no. 3, pp. 396-405, May 2017, DOI: 10.1109/TNANO.2017.2677882.

[13] Y. Pang, H. Wu, B. Gao, D. Wu, A. Chen and H. Qian, "A novel PUF against machine learning attack: Implementation on a 16 Mb RRAM chip," 2017 IEEE International Electron Devices Meeting (IEDM), San Francisco, CA, 2017, pp. 12.2.1-12.2.4, DOI: 10.1109/IEDM.2017.8268376.

[14] G. E. Suh, S. Devadas, “Physical unclonable functions for device authentication and secret key generation”, Proceedings of the 44th ACM/IEEE Design Automation Conference 2007, pp. 9-14.

[15] C. Herder, M.D. Yu, F. Koushanfar, S. Devadas, “Physical Unclonable Functions and Applications: A Tutorial”, Proc. IEEE 102 (2014) 1126-1141, DOI: 10.1109/JPROC.2014.2320516.

[16] A. Chen, “Comprehensive assessment of RRAM-based PUF for hardware security applications,” in IEDM Tech. Dig., Dec. 2015, pp. 265–268, 10.1109/IEDM.2015.7409672.

[17] M. Wu et al., "A PUF scheme using competing oxide rupture with bit error rate approaching zero”, IEEE International Solid - State Circuits Conference - (ISSCC), San Francisco, CA, 2018, pp. 130-132 DOI: 10.1109/ISSCC.2018.8310218

[18] G.S. Rose, J. Rajendran, N. McDonald, R. Karri, M. Potkonjak, B. Wysocki, “Hardware security strategies exploiting nanoelectronic circuits” Proceedings of the 18th Asia and South Pacific Design Automation Conference (ASP-DAC) 2013, pp. 368-372, DOI: 10.1109/ASPDAC.2013.6509623.

[19] S. Balatti, S. Ambrogio, R. Carboni, V. Milo, Z. Wang, A. Calderoni, N. Ramaswamy, D. Ielmini, “Physical unbiased generation of random numbers with coupled resistive switching Devices” IEEE Trans. Electron Devices 63 (2016) 2029-2035, DOI: 10.1109/TED.2016.2537792.

[20] D. Arumi, M.B. Gonzalez, F. Campabadal, “RRAM serial configuration for the generation of random bits”, Microelectronic engineering (2017), vol. 178, p. 76-79, DOI10.1016/j.mee.2017.04.043.

[21] D. Arumi, S. Manich, R. Rodríguez-Montañés, “RRAM based cell for hardware security applications” Proceedings of the 1st IEEE International Verification and Security Workshop (IVSW) 2016, pp. 1-6, DOI: 10.1109/IVSW.2016.7566599.