RRAM Serial Configuration for the Generation of Random Bits

D. Arumí[1], M. B. González[2], F. Campabadal[2]
[1]Universitat Politècnica de Catalunya-Departament d'Enginyeria Electrònica, 08028, Barcelona, Spain
[2]Institut de Microelectrònica de Barcelona. IMB-CNM (CSIC), 08193, Bellaterra, Spain
daniel.arumi@upc.edu

Abstract

In this work the serial combination of two RRAM cells is studied for the generation of a random bit. Measurements confirm that a serial reset operation, in which one of the two RRAMs switches to the high resistance state, is an unpredictable and random process. Furthermore the same device switches during subsequent set and reset operations. This behavior paves the way for the application of this configuration for hardware security purposes.

***Keywords*— Resistive Random Access Memory (RRAM), random bit, Physical Unclonable Function (PUF), hardware security, serial configuration.**

1. Introduction

The stochastic switching mechanism of RRAMs (Resistive Random Access Memories) generates intercell and cycle-to-cycle variability, with significant impact in device resistance [1]. This phenomenon can be exploited for random bit generation. In fact, RRAM is positioning as one of the most promising candidates for hardware security applications. Some recent works have explored the feasibility of these devices in PUFs (Physical Unclonable Functions) intended for device authentication and secret key storage purposes [2]-[9]. A PUF [10]-[11] is a security primitive which embraces manufacturing variations resulting from the fabrication process to derive a secret from the physical characteristics of integrated circuits (ICs). In a reliable application, a PUF must produce uniformly distributed, independent and robust random bits. Therefore, similar to traditional silicon based PUFs, RRAMs enable extracting a hardware intrinsic secret from variability.

This works investigates the behavior of a primitive composed of two RRAMs serially connected to extract a secret. Although this configuration has already been proposed for TRNGs (True Random Number Generators) [12]-[13], the present works exploits its potential use for PUFs applications.

2. Sample description

TiN/Ti/HfO_2/W devices were fabricated with a field oxide isolation scheme. A 10nm-thick HfO_2 layer was deposited by atomic layer deposition (ALD) at 225ºC using TDMAH and H_2O as precursors. The top and bottom 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.1a shows a schematic cross-section of the final device structure. The resulting structures used in the experiments are square cells of 15x15μm^2 (see Fig. 1b). The resistive switching mechanism in this type of devices is attributed to morphological and stoichiometric changes of oxygen deficient conductive filaments [14].

3. Results and discussion

The electrical characterization of the devices was performed using a Keysight B1500 semiconductor parameter analyzer. In order to automatically perform measurements, the B1500 instrument was connected to a computer via GPIB and controlled using MATLAB.

First, the resistive switching behavior was assessed under DC. The voltage was applied to the top electrode while the bottom electrode was grounded. 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. As expected, in the high resistance state (HRS) cycle-to-cycle variability is larger than in the low resistance state (LRS).

After that, voltage pulses were programmed and applied to the devices in order to evaluate the resistive switching behavior in the pulse mode.

For a single device (Fig 3.a), the waveform applied during cycling is shown in Fig 3.b. Note that the same voltage amplitudes as in the case of DC were used for the switching operations. The corresponding cycling behavior is shown in Fig 4.

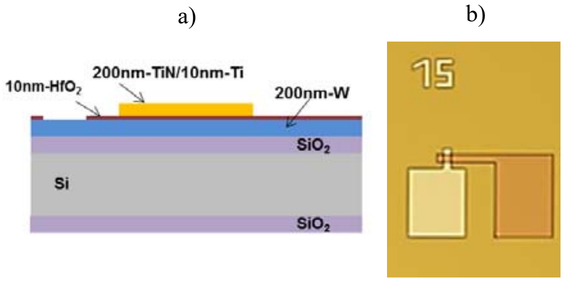

Fig.1: a) Schematic device cross-section b) Top view optical microscope image.

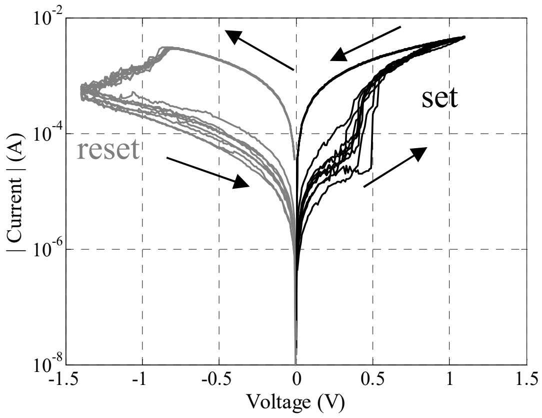

Fig.2: Resistive switching behavior during successive set and reset operations.

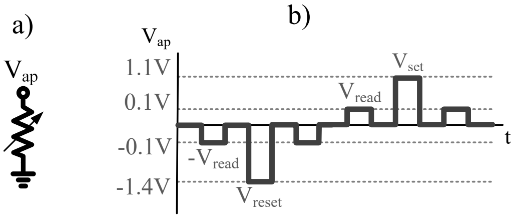

Fig.3: a) Schematic device configuration b) Diagram of the applied voltage pulses.

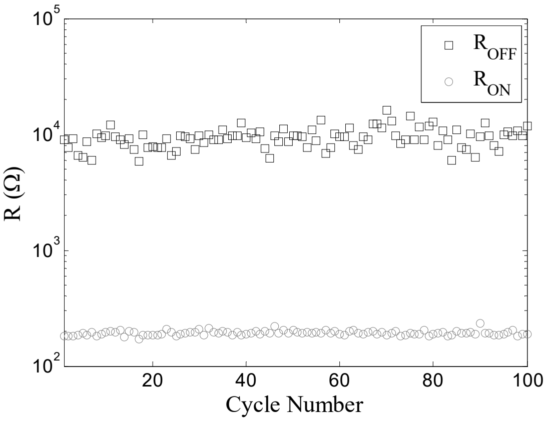

Fig.4: R_{OFF} and R_{ON} resistances during cycling for a single RRAM.

The proposed serial configuration of two RRAMs for the generation of a random bit is depicted in Fig. 5a. The bottom electrode of the top RRAM (R_{top}) is connected to the top electrode of the bottom RRAM (R_{bottom}). The voltage pulses were applied to the top electrode of R_{top}, as depicted in Fig 5b. The bottom electrode of R_{bottom} was grounded whereas the common terminal of the two devices was left floating. Notice that the voltage amplitudes in the serial configuration were adjusted as to have similar values as for a single device. They are high enough to trigger the device switching but avoiding its degradation. The experimental serial set-up comprised the application of numerous sequential pulses.

During a first serial reset operation, one of the RRAMs switches to the HRS. When the reset is initiated, the voltage across the switching device increases, preventing the other device to switch. The RRAM that goes first to the HRS is unpredictable and this behavior can be exploited as the source of randomness. During a subsequent serial set operation, only the RRAM at the HRS switches, since the other one is already at the LRS. Experimental evidence of this behavior is shown in Figs. 6 and 7, where the resistances of two serial RRAMs are plotted after every reset and set operation, respectively. In this particular example, after a reset, R_{top} switched to the HRS, whereas R_{bottom} remained at the LRS.

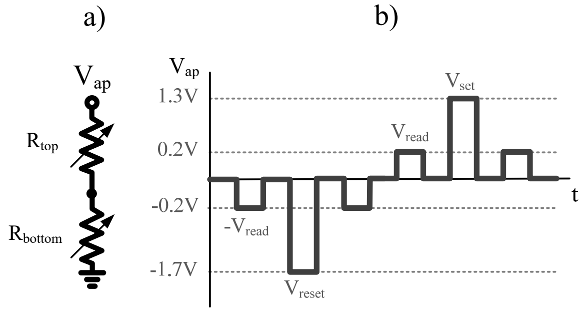

Fig.5: Serial configuration a) Schematic b) Diagram of the applied voltage pulses.

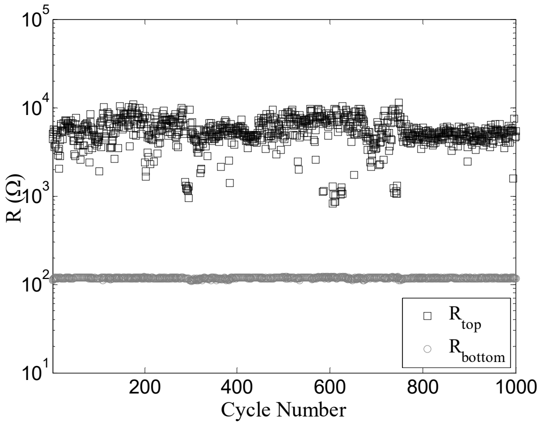

Fig. 6: Resistances of the RRAMs pair during cycling after a serial reset operation.

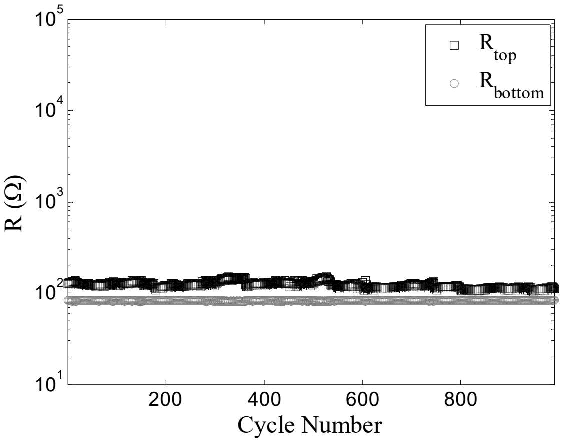

Fig. 7: Resistances of the RRAMs pair during cycling after a serial set operation.

Similar experiments were performed with other RRAMs pairs, where only one of the two devices was found to switch during consecutive set/reset operations. A summary of the results for different RRAMs pairs is given in Fig. 8. The reported average resistances for R_{top} and R_{bottom} after a serial reset indicates that the switching device can be either of the two devices, indistinctly.

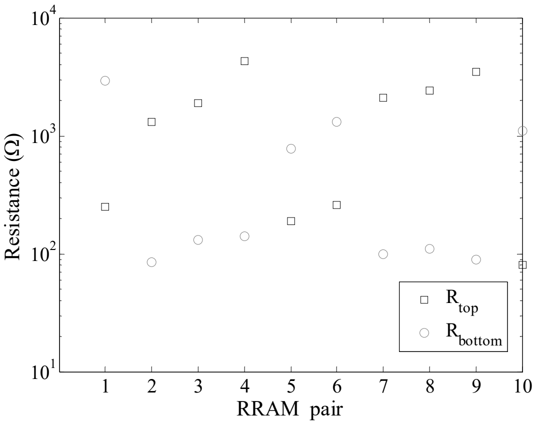

Fig. 8: Average resistance for R_{top} and R_{bottom} after a serial reset for different RRAMs pairs, where more than 300 serial pulse sequences were considered.

4. Conclusions

The reset of two serially connected RRAMs generates an unpredictable switch of one of the devices. The switching of this device persists for subsequent set and reset operations whereas the other RRAM remains in the low resistance state. This configuration can be employed for the generation of random bits, which can be obtained by reading either one of the two RRAMs after a reset operation. Hence, this primitive can be leveraged for the implementation of PUFs in hardware security applications. Furthermore, due to the robustness shown during cycling, serial set operations, resulting in both RRAMs in the low resistance state, can obfuscate the secret, preventing the potential vulnerability of reading out the secret after powered down.

Acknowledgements

This work has been partially supported by the Spanish Ministry of Economics and Competitiveness, projects references TEC2013-41209-P, TEC2014-52152-C3-1-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, *IEDM 2011*, pp. 413-416.

[2] J. Rajendran, G.S. Rose; R. Karri; M. Potkonjak, *ISVLSI 2012*, pp. 84-87.

[3] J. Rajendran; R. Karri; J.B. Wendt; M. Potkonjak; N. McDonald; *et al*, *Proc. IEEE* 103 (2015) 829-849.

[4] A. Chen, IEEE EDL, vol.36, (2015), pp.138-140.

[5] R. Liu, H. Wu, Y. Pang, H. Qian, S. Yu, IEEE EDL 36 (2015), pp.1380-1383.

[6] A. Mazady, M.T. Rahman, D. Forte, M. Anwar, IEEE ETCAS 5 (2015), pp.222-229.

[7] C. Pai-Yu, F. Runchen, L. Rui, C. Chakrabarti, C. Yu, Y. Shimeng, *IEEE HOST 2015*, pp.26-31.

[8] D. Arumi, S. Manich, R. Rodríguez-Montañés, *IVSW, 2016*,1-6

[9] Y. Pang, H. Wu, B. Gao, N. Deng, R. Liu, *et al*., IEEE EDL, vol. 38, (2017), pp. 168-171.

[10] G. E. Suh, S. Devadas, *ACM/IEEE DAC*, 2007, pp. 9-14.

[11] C. Herder, M.D. Yu, F. Koushanfar, S. Devadas, Proc. IEEE 102 (2014) 1126-1141.

[12] G.S. Rose *et al*, ASP-DAC 2013, 368-372.

[13] S. Balatti *et al*., IEEE TED 63 (2016), pp. 2029-2035.

[14] G. Gonzalez-Cordero, et al. J. Vac. Sci, Tech. B 35 (2017) 01A110-1 - 01A110-5