Enhanced serial RRAM cell for unpredictable bit generation

R. Rodríguez-Montañés a,b,*, D. Arumí a, A. Gómez-Pau a, S. Manich a, M.B. Gonzalez b, F. Campabadal b

a Universitat Politècnica de Catalunya, Departament d'Enginyeria Electrònica, 08028 Barcelona, Spain
b Institut de Microeleccència de Barcelona, IMB – CNM (CSIC), 08193 Bellaterra, Spain

ARTICLE INFO

Keywords:
RRAM
Resistive switching
PUF
Hardware security
Unpredictable bit

ABSTRACT

In this letter, the serial configuration of two RRAMs is used as a basic cell to generate an unpredictable bit. The basis of the operation considers starting from the Low Resistive State (LRS) in both devices (initialization step), then, one of them is switched to the High Resistive State (HRS) (bit generation step) without knowing, in advance, which one is the switching device (unmasking step). In this proposal, the larger resistance variability of HRS compared to LRS is considered to improve the masking performance of the cell (masking step). The presented experimental results are a proof-of-concept of the applicability of the proposal.

1. Introduction

The increase in the use of the Internet of Things (IoT) reveals the need of greater protection against security threats. The inherent variability of RRAMs, due to the stochastic nature of their switching mechanism [1], has positioned these devices as one of the most competitive candidates for the development of hardware security applications [2]. In fact, RRAMs have captured the attention of the research community for the implementation of PUFs (Physical Unclonable Functions) [3–7] and TRNGs (True Random Number Generators) [8,9].

PUFs can generate secure information inside a chip based on process variations during semiconductor fabrication [10,11]. Although circuits are manufactured with identical layout design and using the same process conditions, their electrical characteristics differ because of process variability. The present work uses the association of two RRAMs in series as a basic cell for PUFs, able to generate an unpredictable bit [12,13]. In order to mask the generated bit, an additional operation including a masking step has been considered and experimentally evaluated.

The paper is organized as follows. Section II describes the RRAM devices and the experimental setup used in this work. Section III explains the principle of the proposed PUF cell, while Section IV presents the extension of the basic operation of the cell. Experimental results are presented in Section V and, finally, conclusions are drawn in Section VI.

2. RRAM devices

The RRAM devices employed in this work are TiN/Ti/HfO2/W structures [12,13]. A schematic cross-section of the devices is shown in Fig. 1(a) and a top view image of them is illustrated in Fig. 1(b). Different squared cells of 60 × 60 μm2, 15 × 15 μm2 and 5 × 5 μm2 have been used.

The electrical characterization of the devices was performed through serial configuration (see Fig. 2). Measurements were carried out by means of two synchronized Keysight B2912A Precision Source/Measure Units (SMUs) controlled through GPIB using a Matlab script (see Fig. 3).

Both, DC and pulsed measurements were performed on isolated devices. Initially, the resistive switching behavior of the devices was assessed under DC conditions, as shown in Fig. 4(a) for a single device. Different squared cells of 60 × 60 μm2, 15 × 15 μm² and 5 × 5 μm² have been used.

The corresponding cycling behavior for pulsed measurements was subsequently evaluated, Fig. 4(b).

Once the independent operation of two RRAMs was validated, the experiments with the serial RRAM cell were conducted as presented in the next section.

3. Basic RRAM serial configuration

The structure of two RRAM devices connected in series has been proposed as an unpredictable bit generator cell [12]. Its operating
The principle starts with both devices in LRS (Fig. 5). In order to generate the bit, a serial RESET voltage ($V_{S,\text{RESET}}$) able to switch any of the devices from LRS to HRS is applied. Once one of the RRAMs has switched to HRS, the current flowing through the serial structure decreases and the other device remains in LRS. It is not possible to know which one of the devices is going to switch in advance, which makes the generated bit unpredictable. Measuring the voltage at the middle point ($V_M$) allows the reading of the generated bit. In order to mask the outcome of the cell, a SET voltage ($V_{S,\text{SET}}$) is applied afterwards, causing both devices to go back to the initial LRS.

![Fig. 1.](image1.png)

**Fig. 1.** (a) HfO$_2$-based RRAM cross-section (b) Top view optical microscope image of three squared RRAM devices in a cross-point configuration with different areas ($60 \times 60 \, \mu m^2$, $15 \times 15 \, \mu m^2$ and $5 \times 5 \, \mu m^2$) and their access pads.

![Fig. 2.](image2.png)

**Fig. 2.** (a) Top ($R_T$) and bottom ($R_B$) RRAMs are accessed through their Top (Ti) and Bottom (Bi) electrode pads (b) Nodes are connected to channels $Ch_{jk,p}$ ($j$ indicates the instrument, $k$ the channel and $p$ the pad).

![Fig. 3.](image3.png)

**Fig. 3.** Experimental setup where devices M1 and M2 are serially connected and individually formed and characterized.

![Fig. 4.](image4.png)

**Fig. 4.** (a) DC resistive switching behavior during successive SET and RESET operations (b) $R_{\text{LRS}}$ and $R_{\text{HRS}}$ resistances during pulsed SET and RESET operations.

![Fig. 5.](image5.png)

**Fig. 5.** Transitions between the initialization step (both RRAMs are in LRS) and the bit generation step (one of the devices is in HRS).
For a given pair of devices, it is during the first RESET operation where the unpredictable bit is generated. The application of the subsequent serial SET and RESET operations results in a repetitive mask and unmask process of the same bit, since the same device is the one switching in subsequent serial SET and RESET operations [12]. In technologies where device-to-device variations are dominant over cycle-to-cycle variations, the prevalence of the same switching device is expected to be stable over time. Furthermore, post-processing could be considered, as the use of Helper Data Algorithms [14] and the use of Error-Correcting Codes [15], to detect and correct pairs of devices not behaving as expected.

In [12], the initial step of the cell uses the LRS of both RRAM devices for masking the unpredictable bit. The variability observed in LRS is much smaller than in HRS (see Fig. 4). Therefore, masking at HRS is expected to offer better protection than at LRS.

4. Extended RRAMs serial configuration

With the aim of improving the masking features of the cell, the addition of a third step that takes advantage of the wide resistance variability of RRAM devices at HRS is proposed and evaluated.

The new step is added as shown in Fig. 6 where this masking phase is illustrated. After unmasking the bit (Bit generation step), both RRAM devices are switched to HRS.

![Fig. 6. Extended operation for the serial RRAM cell. After initialization and bit generation steps, the addition of the masking step leads to both devices to the HRS.](image)

![Fig. 7. Voltage pulses for the proposed sequence of operations including a compensation step to balance the positive and negative voltages applied to each device.](image)

![Fig. 8. Example #1: experimental $R_T$ and $R_B$ after (a) initialization, (b) bit generation and (c) masking steps. (d) Cumulative probability of $R_T$ and $R_B$ at the initialization step (both at LRS) and at the masking step (both at HRS).](image)
devices are brought to HRS instead of LRS. So that the masking is kept at this HRS in which the higher variability of resistances is exploited. Before unmasking the bit once again, both RRAM devices are switched to LRS (Initialization step) and, then, the serial RESET is applied (Bit generation step). These three steps can be repeated any number of times following the same sequence. Notice that in the “Initialization” and “Masking” steps the RRAM devices are switched independently (not in series). This is accomplished by grounding the VM node.

To keep the expected switching characteristic of the devices, they must undergo balanced set/reset operations to avoid the accumulation of too many oxygen vacancies at one side of the bilayer structure which would lead to the device failure [16]. However, with the addition of the masking step, each RRAM would undergo 2 negative voltage pulses versus only one positive. To solve these unbalanced excitations, a compensating step is added as illustrated in Fig. 7.

5. Experimental results

In this section, the experimental measurement results for three representative cases are presented. The measured resistances after initialization, bit generation and masking operations are detailed. Resistances for the compensation step have been found to be very similar to those of the initialization step.

Fig. 8 illustrates the first example where both devices start from LRS (Fig. 8a). After a voltage pulse allowing their serial transition to HRS (Bit generation), only the bottom device has switched to HRS as shown in Fig. 8(b). Before applying the masking step, the compensation step (not shown in Fig. 8) causes both devices to have a very similar distribution of resistances as in the initialization step. Then, in the masking step both devices end up at HRS (see Fig. 8c). The cell remains in the masking step as long as a new bit generation cycle is required, making it difficult for an external attacker to know the stored bit due to the wide range of RT and RB variability in the resting HRS state. Notice that the comparison of HRS values between the top and the bottom RRAMs does not give any clue about the unpredictably generated bit since their resistance distributions completely overlap (Fig. 8d).

Fig. 9 and Fig. 10 illustrate two more examples of the application of the proposed methodology to generate one unpredictable bit. In the former, the device switching is RB and, in the masking step, RB is clearly higher than RT. In the latter, the switching device is the RT while, in the masking step, its resistance is lower than the non-switching device.

6. Conclusion

The serial configuration of two RRAMs has been considered to generate unpredictable bits. To improve the masking performance of the cell, both devices are forced to the HRS in the masked state. Experimental evidence of this behavior is reported for three representative examples, showing that the proposed cell may be leveraged for a PUF-like application.

Declaration of Competing Interest

The authors declare that they have no known competing financial
interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

This work was supported in part by the Spanish Ministry of Science, Innovation and Universities under Grant PID2019-103869RB-C33/AEI/10.13039/501100011033, and through FEDER funds under Grant TEC2017-84321-C4-1-R.

References


Rosa Rodríguez-Montañés received the M.S. degree in physics from the Universitat de Barcelona in 1988 and the Ph.D. degree from the Universitat Politècnica de Catalunya (Barcelona, Spain) in 1992. Since 1994, she has been an Associate Professor with the Department of Electronic Engineering at UPC. Her research interests include defect characterization and defect diagnosis of digital nanometric CMOS technologies, hardware security and emerging technologies.

Daniel Arumí received the M.S. degree in industrial engineering and the Ph.D. degree in electronic engineering from the Universitat Politècnica de Catalunya (UPC), Barcelona, Spain, in 2003 and 2008, respectively. He is currently an Associate Professor with the Department of Electronic Engineering, UPC. His current research interests include hardware security, emerging technologies, defect-based testing, fault modeling and defect diagnosis.

Álvaro Gómez-Pau received the M.Sc. degree in Engineering from Universitat Politècnica de Catalunya (UPC-BarcelonaTech) and the Ph.D degree in Electronics Engineering from the same university in 2010 and 2017, respectively. He is a researcher and an assistant professor at the Electronics Engineering Department at UPC. During his Ph.D., he was a visiting scholar at Georgia Institute of Technology, Atlanta, Georgia, USA and University of Eindhoven, Eindhoven, The Netherlands. His research interests focus on test, diagnosis, robustness and reliability of nonvolatile memory devices and their applications to secure systems. Álvaro Gómez has been an IEEE Member since 2012.

Salvador Manich received the M.Sc. degree in Industrial Engineering in 1992 and Ph.D. in Industrial Engineering in 1998 at the UPC. He is associate professor since 2001 in the school of Industrial Engineering and member of the Electronic Engineering department. He develops his research activity in the Quality in Electronics group (QinE) and he is also a member of the Center for Research in Nanoe ngineeringing (CRNE). He has been an invited researcher in the IST (Portugal) and TUM (Germany). His main research interests are low-power design, test of digital systems and security in hardware structures.

Mireia Bargallo Gonzalez received the degree in physics from the University of Barcelona, Barcelona, Spain, and the Ph.D. degree on the topic of stress analysis and defect characterization techniques of semiconductor materials and devices, from Katholieke Universiteit Leuven, Leuven, Belgium, in 2011. She pursued her Ph.D. thesis with the Interuniversity Microelectronics Center (imec), Leuven, Belgium. In 2011, she joined the Institut de Microelectrónica de Barcelona (IMB-CNM, CSIC). Her current research interests include electrical characterization, modeling and applications of resistive switching devices.

Francesca Campabadal received the Ph.D. degree in physics from the Universitat Autònoma de Barcelona, Bellaterra, Spain, in 1986. She joined the Institut de Microelectrónica de Barcelona, Consejo Superior de Investigaciones Científicas, Barcelona, Spain, in 1987, where she is currently a Research Professor. Her current research interests include the deposition of high-k dielectric layers, their electrical characteristics, and the resistive switching phenomena in RRAM devices.