RRAM Based Random Bit Generation for Hardware Security Applications

Daniel Arumí[1], Salvador Manich[1], Rosa Rodríguez-Montañés[1], Michael Pehl[2]
[1]Universitat Politècnica de Catalunya - Departament d'Enginyeria Electrònica, Barcelona, Spain
[2]Technische Universität München, Munich, Germany

Abstract— Resistive random access memories (RRAMs) have arisen as a competitive candidate for non-volatile memories due to their scalability, simple structure, fast switching speed and compatibility with conventional back-end processes. The stochastic switching mechanism and intrinsic variability of RRAMs still poses challenges that must be overcome prior to their massive memory commercialization. However, these very same features open a wide range of potential applications for these devices in hardware security. In this context, this work proposes the generation of a random bit by means of simultaneous write operation of two parallel cells so that only one of them unpredictably switches its state. Electrical simulations confirm the strong stochastic behavior and stability of the proposed primitive. Exploiting this fact, a Physical Unclonable Function (PUF) like primitive is implemented based on modified 1 transistor – 1 resistor (1T1R) array structure.

Keywords—RRAM, PUF, security, stochastic switching, hardware security, variability, memory array

I. Introduction

An RRAM (Resistive random access memory) is typically composed of an electrode/dielectric/electrode stack structure. Its physical mechanism relies on formation and rupture of conductive filament (CF) with defects in oxide (dielectric) between the two metal electrodes [1]. For a fresh RRAM, an initial operation, called the forming process, is usually required to generate the CF. The forming process is critical since it determines the CF characteristics, which in turn influence RRAM performance. Once the CF is formed, an RRAM can reversible switch between a high-resistance state (HRS) and a low-resistance state (LRS). This switching behavior is obtained applying voltage pulses between the electrodes. The switching operation from HRS to LRS is called the set process. On the contrary, the switching operation from LRS to HRS is called the reset process.

Due to the randomness of the defect generation and annihilation, the shape of the CF presents variability from cell to cell and also from cycle-to-cycle, with significant impact in the resistance of the device [2]-[4]. Hence, this stochastic switching mechanism still poses challenges that must be overcome prior to the massive commercialization of RRAM memories. Nevertheless, the very same challenges have positioned these devices as a promising alternative for the development of hardware security applications [5]. In fact, special interest is focusing on Physical Unclonable Function (PUFs), security primitives which embrace manufacturing variations resulting from the IC fabrication process for authentication and secret key storage purposes [6]-[7].

This paper proposes to use RRAMs as a hardware intrinsic security feature which is similar to PUFs. A preliminary work can be found in [8]. The proposal is implemented in a 1 transistor – 1 resistor (1T1R) array. It improves over state-of-the-art by integrating parts of the quantization, which is required to generate a secret bit, into the design of the RRAM. The rest of the work is organized as follows. The works related with RRAM based PUFs is reviewed in Section II. Section III briefly explains the basis of 1T1R array. Section IV proposes a cell structure based on two parallel RRAMs to derive a random bit. The PUF-like implementation is presented in Section V. Section VI summarizes the electrical simulations results confirming the feasibility of the proposal. Finally, the conclusions of the work are given.

II. RRAMs for Hardware Intrinsic Security

Emerging memories are attracting the attention of the research community for security applications. Although recent works have appeared based on RRAM [9]-[21] and STT-MRAM (Spin Transfer Torque Magnetic RAM) [22]-[24] technologies, RRAM is positioning as the most promising candidate for these applications. Just like traditional silicon based PUFs, RRAMs allow extracting a hardware intrinsic secret from process variations. The secret does not depend on a configuration which is selected by a challenge. Thus, the concept is similar to a so-called weak PUF [7]. Such primitives are typically used to derive a unique key which is inseparably connected to hardware. In case of RRAMs, this key only depends on variations in the CF, which is reflected by a cell-specific switching characteristic from HRS to LRS and vice versa. The state (HRS or LRS) is kept after power off.

The permanent storage of a value in form of a specific resistance of a certain RRAM cell together with the derivation of the secret from hardware intrinsic variations, places RRAMs at the border between traditional PUFs and non-volatile

978-1-5090-4565-5/16/$31.00 ©2016 IEEE

memories (NVMs). Since RRAMs are a type of NVM they have the potential vulnerability to be read out after powered down. However, due to the small size of the cells (approx. 10 nm size square) and since the RRAMs are embedded between metal layers, it is expected that it will be hard to read out in practice. However, this attack vector has to be considered in future and might require adding some countermeasures to achieve a high level of security. But the NVM-characteristic of RRAMs, which is well suited to reliably store information, also adds a benefit. A traditional PUF which is used for key storage requires strong error correction to reduce the expected bit error probability of the PUF (typically 15% to 25% per bit) to an acceptable key error probability of 10^{-6} to 10^{-9} per key. A more reliable primitive would allow reducing the overhead during runtime and in hardware. Another feature of RRAMs which might be used in future is that the secret stored in the RRAM cells can easily be erased permanently by applying a high voltage pulse. This can enable many additional applications for RRAM based security primitives in the future.

To derive a secret from an RRAM, the most common approaches are based on 1T1R array structures. In [9], initially all cells are put to the same resistance state (HRS or LRS). Two sensing modes are proposed to obtain random bits: the first compares the resistance of one cell against a reference cell and the second, which is reported to derive betters results, pairwise compares the resistances of two cells. The secret in these approaches is extracted by, in the first case, detecting if the resistance is above or below a certain threshold and, in the second case, looking at which of the cells has higher or lower resistance. Chen [10] extends the second approach from [9] by applying two n-bit words, which are used to select two times n RRAM cells. An n bit response is received by bit-wise comparison. In [11] the cells are first set to LRS and then a weak reset operation is applied, so that every cell has 50% of probability to switch to HRS. Instead of comparing RRAM cells, the experimental work in [12] selects a reference current so that for 50% of the cells the current is higher and for the rest 50% the current is lower than the reference when they are measured during the read operation. As dummy cells are leveraged to derive this reference, this concept is similar to the first sensing mode described in [9].

Purely passive (without transistors) crossbar array architectures have also been examined for PUF applications. The authors in [13] presented a preliminary work based on memristors. Weak write operations, i.e. shorter pulse widths and lower voltage amplitudes, are analyzed for the generation of random bits. The crossbar array was leveraged to build a public PUF (PPUF) in [14].

Pai-You et al. [15] increase the number of bits extracted from an array by selecting pairs of cells from different columns. By comparing the resulting currents through the activated cells secret bits are obtained.

Particular cell topologies are specifically designed for security applications. In [16] a cell composed of two RRAMs in series was postulated as the source of random bit generation. Starting both RRAMs in LRS, a reset operation is applied to them. The inherent variability of the switching mechanism causes one of the two RRAMs to become first high resistive, forcing the other RRAM to remain in LRS. Experimental evidence of this fact was presented in a subsequent work [17]. The recent work in [18] extend the analysis to different coupling configurations of two RRAM devices as the source for random bit generation.

It is worth mentioning that RRAMs have also been proposed as true random number generator (TRNG) for applications in data encryption for secure communication systems [19]-[21].

Although the research community is pushing towards RRAM based PUF-like structures, proposals still do not meet all desired requirements. 1T1R approaches are mainly restricted by the limits of sense amplifiers and crossbar arrays must handle the sneak path issue (currents that flow through other RRAMs rather than the target).

The proposal in this work improves the 1T1R by integrating parts of the quantization for secret bit generation into the RRAM design. Thus, it is able to derive bits comparing quite different LRS and HRS resistances so that no additional performances are demanded from the sense amplifier. Simulation results show high random quality of the generated bits.

III. 1T1R ARRAY

There are mainly two array architectures for RRAM integration: the 1T1R and the crossbar. The former offers better write/read margins and has a bigger array size whereas the latter shows smaller cell area and lower power consumption. This work exploits the use of 1T1R arrays. Thus, from here on the focus is on this architecture.

In a 1T1R array, see Fig. 1, each RRAM device is connected in series with a cell selecting transistor. Based on these primitives, the array is composed of word lines (WLs) connecting the gate terminals in the same row, bit lines (BLs) connecting RRAMs of the same column, and source lines (SLs) connecting the source terminals of transistors in the same column. Source lines are usually connected to ground (cf. Fig. 2.a). Transistors in 1T1R cells select each specific cell independently from the others.

A write operation is performed by applying a voltage V_{WL} to the WL (this selects the cell) and simultaneously a second voltage (V_{SET} or V_{RESET}) to the corresponding BL. This is illustrated in Fig. 2.b and 2.c. Assuming a bipolar RRAM, a positive voltage ($V_{SET} > 0$) or a negative voltage difference ($V_{RESET} < 0$) between the top electrode (TE) and bottom electrode (BE) is required to conduct a set or a reset operation.

For the read operation, a cell is selected by connecting the corresponding WL to the voltage V_{WL} and the corresponding BL to the read voltage V_{READ}. The logical value stored in the cell is determined by a sense amplifier that is connected to the bit line and who measures the current of the RRAM when V_{READ} is applied. Notice, that V_{READ} is a small fraction of the voltage applied during a set operation.

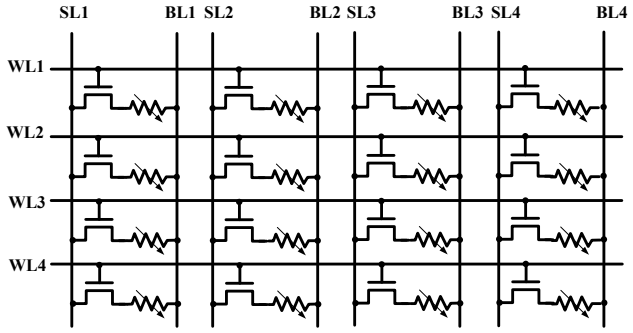

Fig. 1. 4x4 1T1R array.

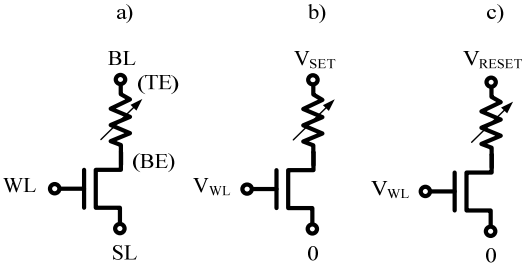

Fig. 2. a) 1T1R cell b) Set operation c) Reset operation.

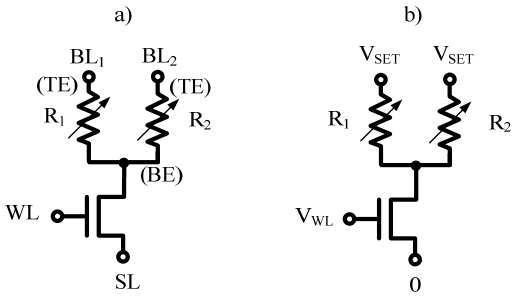

Fig. 3. a) Cell topology for a random bit generation b) Simultaneous set operation.

IV. Secret Bit Generation

A configuration with two 1T1R cells is considered for the generation of a secret bit. Initially, the TEs of the resistive elements are connected to different BLs. The BE nodes of the two cells are connected so that the transistors of the two 1T1R cells are merged in parallel behaving like a single transistor. This results in an 1T2R cell (cf. Fig. 3.a). Now, the bit-lines are virtually connected and next a simultaneous set operation (SSO) is performed for the two RRAMs by applying a voltage V_{SET} to both BLs (cf. Fig. 3.b). The transistor's source terminal is grounded and a positive voltage (V_{WL}) is applied to the gate terminal. Due to the inherent RRAM variability, one of the devices switches first from HRS to LRS while the other remains HRS.

For instance, assume that R_2 switches first to LRS. Then, BE voltage will increase due to the higher current passing through R_2 and the voltage divider composed of the parallel RRAMs and the selecting transistor. As a consequence, the current flowing through R_1 will abruptly decrease avoiding the complete set process of the CF in R_1 which will remain in HRS. Which of the RRAMs (R_1 or R_2) goes first to LRS and prevents the other from the CF set process is unpredictable and is exploited as the source of randomness.

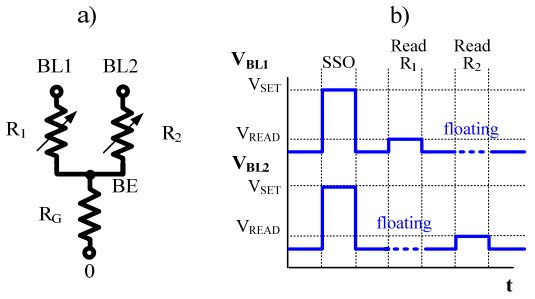

Fig. 4. Experiment a) Circuit topology b) Sequence of applied stimulus.

TABLE I
PARAMETER VALUES OF THE EXPERIMENT

Parameter		Value
Bit line voltage for a set operation (V)	V_{SET}	0.9
Bit line voltage for a reset operation (V)	V_{RESET}	-0.7
Bit line voltage for a read operation (V)	V_{READ}	0.2
Resistance (kΩ)	R_G	51

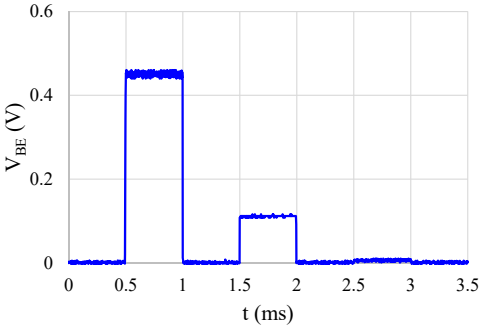

Fig. 5. Experimental behavior of the common bottom electrode (BE) for a random bit generation.

A secret bit can be extracted from the array by addressing either one of the two RRAMs of the 1T2R cell and reading its resistance. During the read operation, the TE of the non-read device must remain disconnected (high-impedance). In larger arrays, multiple response bits of 1T2R cells which are connected to the same word line can be read out in parallel.

The transistors' dimensions must be selected so that their equivalent resistances induce a sufficient voltage drop once the first RRAM switches from HRS to LRS. This must guarantee a big enough current cut in the second RRAM such that it prevents from changing to LRS. An experimental validation of the proposed topology has been performed with chalcogenide-based memristors [25]-[26]. The details of the experiment are shown in Fig. 4, where the transistor has been replaced by a resistance (Fig. 4a). The characteristics were measured using a B2912A SMU and a TDS1002B oscilloscope. The stimulus applied to the circuit are illustrated in Fig. 4b. Starting with both memristors in HRS, a SSO is applied followed by two read operations, one for each memristor. During a read operation, the top electrode of the memristor, which is not read, is kept floating. Table I summarizes the values of the main parameters considered during the experiment. The behavior of the common bottom electrode (BE) is plotted in Fig. 5. During the SSO, one of the memristors switches its state, leading BE to an intermediate voltage. Afterwards, the read operations show that

R_1 is the memristor which has switched to LRS. The equivalent resistances after the SSO are R_1 = 40 kΩ and R_2 = 1.6 MΩ. Notice how there is more than one order of magnitude between them. This is consistent with the expectations for the technology.

The proposed primitive has two advantages when compared to the serial configuration presented in [17]. Firstly, the set operation that generates the random bit is more abrupt than the corresponding reset operation required by the serial configuration. This decreases the probability that the two competing RRAMs end up with the same resistance. Secondly, the proposed primitive is easier to be implemented in existing memory arrays, as it is shown in the next section.

V. Extracting a Secret from an 1T1R Array

This section shows how a 1T1R array must be modified to extract hardware intrinsic secrets using 1T2R primitives. The 1T1R array architecture must be slightly modified to connect two parallel RRAMs and enable the SSO. For this purpose, new connections between adjacent transistors from the same row are added. Like described above, the 1T2R cell is derived from two 1T1R cells which are connected in parallel. Since the source lines are always connected to ground, the two parallel transistors act as an equivalent single one. To implement this behavior in the array, the drains of pairs of transistors in the same row are connected to the same WL (connection highlighted in blue in Fig. 6).

Note that using pairs or transistors has the benefit that it reduces the asymmetries of the design, which in turn minimizes correlations between secret bits, a potential weakness that could be exploited by an attacker. Also note that the inclusion of extra connections implies a modification of the initial memory structure. The most popular method to integrate the RRAM structures is the backend of line (BEOL). Depending on the particularities of the process, these connections may derive different implications in the layout, which should be considered during the design process.

The structure behaves like the circuit shown in Fig. 3.a. and Fig. 6 also illustrates how a SSO can be applied in the modified array. It consists of selecting the common WL for both transistors and applying V_{SET} to both BLs. If required, multiple SSOs can be done in the same row if more BLs are activated. Once the SSOs are applied to the whole memory cells the write operations must finish. During the normal operation of the PUF-like primitive, only read operations are performed. This has advantages in terms of reliability because the small amplitude of the voltage pulse that is applied minimizes the cycle-to-cycle variability.

Secret can be obfuscated to increase the difficulty for a potential attacker to read the cell by resetting the corresponding RRAMs. First, the WL is activated with the voltage V_{WL} and then BL_1 and BL_2 are polarized with the voltage V_{RESET}. Since, the low resistance RRAM will drive most of the current it will quickly reverse his resistance back to HRS, bringing the cell to the initial state with the two RRAMs in HRS.

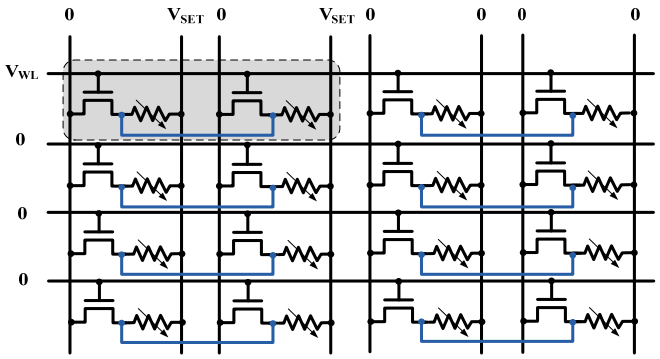

Fig. 6. Example of a SSO. 1T2R cell highlighted in grey.

VI. Experimental Results

Electrical simulations were performed with SPICE to evaluate the proposed PUF-like primitive [8]. MATLAB was used for data processing. A 1T1R array architecture with 256 x 256 cells was built and modified to contain the 1T2R cells giving a total of 32768 1T2R cells. The RRAM model was selected from [27], where the switching mechanism relies on the dynamics of one-dimensional CF growth in the oxide layer. The selecting transistor was implemented in 65nm PTM technology model [28] with minimum length and a width of one and a half times the transistor length. Table II summarizes the values of the rest of parameters considered during simulations.

TABLE II
Parameter Values of the Simulations

Parameter		Value
Array size		256x256
Bit line voltage for a set operation (V)	V_{SET}	2.5
Bit line voltage for a reset operation (V)	V_{RESET}	-1.9
Word line voltage	V_{WL}	1.2
Bit line voltage for a read operation (V)	V_{READ}	0.1
Source line voltage (V)	V_{SL}	0
Pulse width (ns)		20

Variability was included in transistors and RRAM devices. The main internal variable of the RRAM model is the gap distance (g), i.e., average distance between the TE and the tip of the CF, which has an exponential influence on the RRAM resistance. Furthermore, some fitting parameters included in the model were selected to adjust the variability to match realistic experimental data. With these sources of variability and a context of simulation similar to the one reported in [29], two realistic cumulative distributions for the resistance states were obtained [8]. It must be pointed out that for the nominal case $R_{LRS} \approx 10k\Omega$ and $R_{HRS} \approx 760k\Omega$, which provides almost two orders of magnitude between both resistances. As expected, the HRS distribution is wider than the one corresponding to LRS.

During simulations, every cell of the array was initially programmed to HRS. Subsequently, a sequence of SSOs were applied in such a way that one cell of every pair was expected to switch to LRS. Once the whole array was written, the secret bits were obtained in groups of 128 by reading out the corresponding row addresses. Every bit was the result of a read operation at the left 1T1R cell of each 1T2R cell. A voltage V_{READ} was applied to the corresponding BL line of the left RRAM and the current was measured. The other RRAM BL line was kept at high-impedance state. We simulated 250 arrays

with Monte Carlo to include process variations.

The performance was analyzed by means of the four usual parameters assessing the quality of a PUF: uniformity, uniqueness, robustness and bit-aliasing. Note that more advanced performance measures might have to be used for more detailed analysis in future.

Uniformity evaluates the proportion of 0's and 1's in the PUF response. For an n-bit response, uniformity is computed as the percentage of Hamming weigh with respect to the number of bits as follows:

$$\text{Uniformity} = \frac{1}{n}\sum_{i=1}^{n} b_i \times 100\,\% \qquad (1)$$

where b_i is the i-th bit of the response. The ideal value is 50%.

Uniformity results report that the mean of the distribution is close to the ideal value (μ_{unif} = 49.67 %) and the standard deviation σ_{unif} = 3.16 %. It must be pointed out that a detailed analysis of the results showed that around 0.3 % of the cells reported similar resistances for the RRAM pair (resistance ratio lower than five). This happened when the two RRAMs were almost identical with a very similar switching behavior. This phenomenon induces a proportion of cells where the read operation will always result in logic 0 and is assumed to be responsible for the mean value slower than the optimal one. The frequency of this fact might be tolerable in most practical cases, since a larger number of cells can be used and compression can be applied to get sufficient entropy in a derived and corrected secret. Alternatively, the cells can be found easily by measuring both RRAMs in every cell and XORing the derived bits for the same cell. This would allow eliminating such defects.

Uniqueness represents the ability to distinguish a particular PUF among a set of PUFs of the same class. Uniqueness is calculated as the average inter-chip Hamming distance (HD_{inter}) between the responses from k samples of the same PUF.

$$HD_{inter} = \frac{2}{k(k-1)}\sum_{i=1}^{k-1}\sum_{j=i+1}^{k}\frac{HD(B_i, B_j)}{n} \times 100\,\% \qquad (2)$$

where B_i and B_j are the n-bit responses for samples i and j. The ideal value for $k \to \infty$ is 50%.

For the calculation of (2) we took the 256 responses of 128-bits of an array and combined for the 250 simulated arrays. The HD_{inter} results are closely similar to the uniformity results but now with the distribution statistics of $\mu_{HDinter}$ = 50.04% and $\sigma_{HDinter}$ = 0.12%, which are again close to the ideal uniqueness.

Robustness represents the ability of a PUF to reproduce the same response. Robustness is evaluated as the intra-chip Hamming distance among m different responses B_i:

$$HD_{intra} = \frac{1}{m}\sum_{i=1}^{m}\frac{HD(B_0, B_i)}{n} \times 100\,\% \qquad (3)$$

where B_0 is the response at nominal conditions (without noise). The value for an ideal PUF is 0%.

We have simulated our PUF-like primitive at different temperatures. Starting at room temperature the sequences of SSOs were applied and the read operations were subsequently done to get the responses B_0 from the arrays. These sequences of operations were repeated for each new temperature to get responses B_i and equation (3) was applied to evaluate HD_{intra}, In Fig. 7 this metric is plotted and, as expected, it is seen that the performance decreases with the rise of temperature though it keeps under reasonable low values. However, we have not considered the influence of peripheral circuits, i.e. sense amplifiers, which may be affected by temperature and may have an impact during read operations.

Bit-aliasing estimates the tendency towards 0 or 1 of a particular bit response in several PUFs. It gives information about any systematic or spatially caused bias. Bit-aliasing of the i-th bit of k devices is estimated as the relative Hamming weigh of the response on a certain position over all devices. Its ideal value is 50%.

$$\text{Bit} - \text{aliasing} = \frac{1}{k}\sum_{j=1}^{k} b_{i,j} \times 100\,\% \qquad (4)$$

where $b_{i,j}$ is 1 if bit i of PUF j is 1.

We have evaluated the possible spatial effect of line resistances (R_{line}), as shown in Fig. 8. The results obtained for the 250 simulated arrays are illustrated in Fig. 9 for R_{line} = 2Ω. Every pixel corresponds to the bit-aliasing result of a particular bit according to its position. At a first sight, bit-aliasing is seen randomly distributed along the array which indicates that there is not a significant influence of the position over the generation of a secret bit. However, a slightly spatial trend is noticed related to the routing of BL lines. In the figure, the background color is lighter at the upper side than the lower side of the array. Cells located far away from the voltage sources of BLs (upper part of the array) reported on average lower bit-aliasing values than the ones located at the bottom part. This fact means that there is a slight higher probability for RRAMs in the upper side to remain at HRS values. This issue may be of concern for arrays with a relationship between size and line resistance which may cause a non-negligible voltage drop in cells located far away from the BL voltage sources.

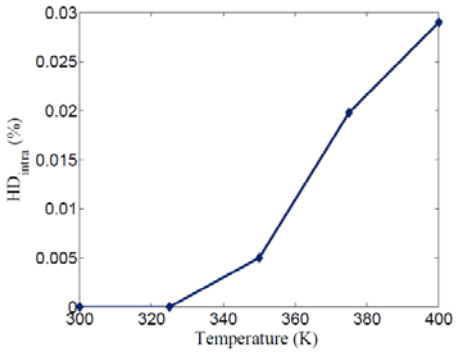

Fig. 7. HD_{intra} results for 256 responses of 128-bits at different temperatures.

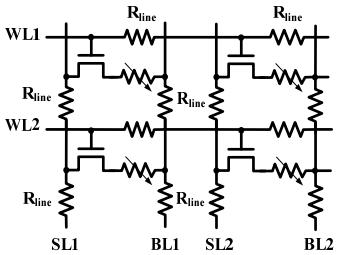

Fig. 8. 2x2 1T1R array including line resistances.

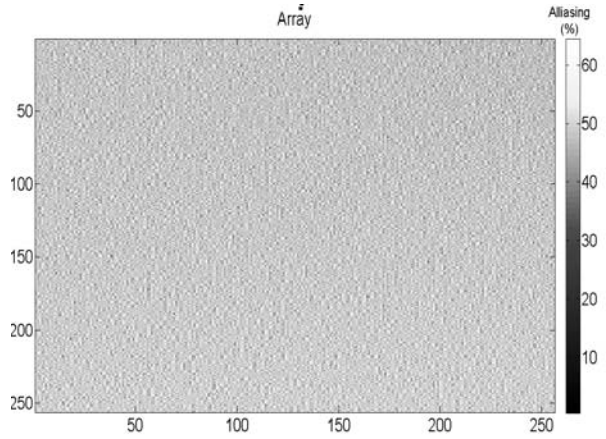

Fig. 9. Bit-aliasing results for $R_{line} = 2\Omega$.

VII. CONCLUSIONS

This work presents a novel PUF-like primitive based on resistive random access memory (RRAM) technology. The inherent variability of the switching mechanism of RRAMs is exploited to generate random (secret) bits. A cell topology is proposed for a regular 1T1R array were slight and regular modifications are introduced. A simultaneous set operation of two RRAMs is used to provoke a chaotic differential unbalance and quantization of the currents required to set them. The subsequent measurement of the resistance in one of the two RRAMs provides the random secret bit. Experimental evidence of this fact is presented. Contrary to state of the art proposals, a regular sense amplifier is sufficient and no additional sensing capabilities are required.

Electrical simulations were performed to analyze the response of the PUF-like primitive in terms of uniformity, uniqueness, robustness and bit-aliasing. The promising results pave the way to continue the exploration of this security primitive in hardware security applications. Future work will be focused on further experimental validation of this proposal.

ACKNOWLEDGMENT

This work has been partially supported by the Spanish Ministry of Economics and Competitiveness, project reference TEC2013-41209-P.

REFERENCES

[1] H.-S.P. Wong et al, “Metal–Oxide RRAM”, Proceedings of the IEEE, vol.100, no.6, pp.1951-1970, June 2012.

[2] A. Chen and M. Lin, “Variability of resistive switching memories and its impact on crossbar array performance,” in Proc. IEEE Int. Rel. Phys. Symp., Apr. 2011, pp. MY.7.1–MY.7.4.

[3] A. Fantini, L. Goux, R. Degraeve, D. J. Wouter, N. Raghavan, G. Kar, A. Belmonte, Y.-Y. Chen, B. Govorea nu, and M. Jurczak , “Intrinsic switching variability in HfO2 RRAM,” in IEEE Int. Memory Work-shop , 2013, pp. 30–33.

[4] M. B. Gonzalez, J. M. Rafi, O. Beldarrain, M. Zabala, andF. Campabadal, “Analysis of the switching variability in Ni/HfO2-based RRAM devices,” IEEE Trans. Device Mater. Rel., vol. 14, no. 2, pp. 769–771, Jun. 2014.

[5] J. Rajendran et al, “Nano Meets Security: Exploring Nanoelectronic Devices for Security Applications”, Proceedings of the IEEE 103(5): 829-849, 2015.

[6] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, ‘‘Silicon physical random functions,’’ in Proc. 9th ACM Conf. Comput. Commun. Security (CCS), 2002, pp. 148–160.

[7] C. Herder, Y. Meng-Day, F. Koushanfar, S. Devadas, “Physical Unclonable Functions and Applications: A Tutorial”; Proc. IEEE, vol. 102, issue 8, pp. 1126-1141, Aug. 2014.

[8] D. Arumi, S. Manich and R. Rodriguez-Montañés, "RRAM based cell for hardware security applications", IEEE International Verification and Security Workshop (IVSW), 2016, pp. 1-6.

[9] Le Zhang; Xuanyao Fong; Chip-Hong Chang; Zhi Hui Kong; Roy, K., "Feasibility study of emerging non-volatilememory based physical unclonable functions," IEEE 6th International Memory Workshop (IMW), pp.1-4, 18-21 May 2014.

[10] A. Chen, "Utilizing the Variability of Resistive Random Access Memory to Implement Reconfigurable Physical Unclonable Functions", IEEE Electron Device Letters, , vol.36, no.2, pp.138-140, Feb. 2015.

[11] A. Chen, “Reconfigurable physical unclonable function based on probabilistic switching of RRAM”; Electronics Letters , vol.51, no.8, pp.615-617, April 2015.

[12] R. Liu, H. Wu, Y. Pang, H. Qian, S. Yu, "Experimental Characterization of Physical Unclonable Function Based on 1kb Resistive Random Access Memory Arrays", IEEE Electron Device Letters, , vol.PP, no.99, pp.1-1, 2015.

[13] P. Koeberl, U. Kocabas¸ and A.-R. Sadeghi. “Memristor PUFs: a new generation of memory-based physically unclonable functions”, Proceedings of the Conference on Design, Automation and Test in Europe . pp. 428-431, March 2013.

[14] J. Rajendran, G. S. Rose, R. Karri, and M. Potkonjak, “Nano-PPUF:A memristor-based security primitive,” in Proc. IEEE Comput. Soc. Annu. Symp. VLSI, 2012, pp. 84–87.

[15] C. Pai-Yu, F. Runchen, L. Rui, C. Chakrabarti, C. Yu, Y. Shimeng, “Exploiting resistive cross-point array for compact design of physical unclonable function", IEEE International Symposium Hardware Oriented Security and Trust, pp.26-31, 5-7 May 2015.

[16] G.S., Rose, J. Rajendran, N. McDonald, R. Karri, R.; M. Potkonjak, M.; B. Wysocki, “Hardware security strategies exploiting nanoelectronic circuits”, Asia and South Pacific Design Automation Conference, pp.368-372, 22-25 Jan. 2013.

[17] A. Mazady, M.T. Rahman, D. Forte, M. Anwar, "Memristor PUF—A Security Primitive: Theory and Experiment". IEEE Journal on in Emerging and Selected Topics in Circuits and Systems, vol.5, no.2, pp.222-229, June 2015.

[18] S. Balatti et al., "Physical Unbiased Generation of Random Numbers With Coupled Resistive Switching Devices", IEEE Transactions on Electron Devices, vol. 63, no. 5, pp. 2029-2035, May 2016.

[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 Electron Device Letters, vol. 33, no. 8, pp. 1108-1110, Aug. 2012.

[20] J. Yang et al., "A low cost and high reliability true random number generator based on resistive random access memory", IEEE 11th International Conference on ASIC (ASICON), Chengdu, 2015, pp. 1-4.

[21] S. Balatti, S. Ambrogio, Z. Wang and D. Ielmini, "True Random Number Generation by Variability of Resistive Switching in Oxide-Based Devices," in IEEE Journal on Emerging and Selected Topics in Circuits and Systems, vol. 5, no. 2, pp. 214-221, June 2015.

[22] L. Zhang, X. Fong, C. H. Chang, Z. H. Kong and K. Roy, "Highly reliable memory-based Physical Unclonable Function using Spin-Transfer Torque MRAM," IEEE International Symposium on Circuits and Systems (ISCAS), pp. 2169-2172, 2014.

[23] A. Fukushima et al., “Spin dice: A scalable truly random number generator based on spintronics,” Appl. Phys. Exp., vol. 7, p. 083001, 2014.

[24] E. I. Vatajelu, G. Di Natale, M. Indaco and P. Prinetto, "STT MRAM-based PUFs," Design, Automation & Test in Europe Conference & Exhibition (DATE), 2015, pp. 872-875, 2015.

[25] A. S. Oblea, A. Timilsina, D. Moore and K. A. Campbell, "Silver chalcogenide based memristor devices”, The 2010 International Joint Conference on Neural Networks (IJCNN), Barcelona, 2010, pp. 1-3.

[26] “KNOWM memristors,” [Online] Available: http://www.knowm.org

[27] X. Guan, S. Yu and H.-S. P. Wong, “A SPICE compact model of metal oxide resistive switching memory with variations,” IEEE Electron Device Letters, vol. 33, no. 10, pp. 1405-1407, 2012.

[28] Predictive Technology Model, http://www.eas.asu.edu/~ptm/

[29] P.-Y. Chen; S. Yu, "Compact Modeling of RRAM Devices and Its Applications in 1T1R and 1S1R Array Design," IEEE Transactions on Electron Devices, vol.62, no.12, pp.4022-4028, Dec. 2015.