





Article

Serial RRAM Cell for Secure Bit Concealing

Binbin Yang ^{1,2}, Daniel Arumí ^{2,*}, Salvador Manich ² , Álvaro Gómez-Pau ² , Rosa Rodríguez-Montañés ² ,
Mireia Bargalló González ³, Francesca Campabadal ³  and Liang Fang ¹

¹ Institute for Quantum Information & State Key Laboratory of High Performance Computing, College of Computer, National University of Defense Technology, Changsha 410073, China; yangbinbin15@nudt.edu.cn (B.Y.); lfang@nudt.edu.cn (L.F.)

² Departament d'Enginyeria Electrònica, Universitat Politècnica de Catalunya, 08028 Barcelona, Spain; salvador.manich@upc.edu (S.M.); alvaro.gomez-pau@upc.edu (Á.G.-P.); rosa.rodriguez@upc.edu (R.R.-M.)

³ Institut de Microelectrònica de Barcelona-Centre Nacional de Microelectrònica, Consejo Superior de Investigaciones Científicas, 08193 Bellaterra, Spain; mireia.bargallo.gonzalez@csic.es (M.B.G.); francesca.campabadal@imb-cnm.csic.es (F.C.)

* Correspondence: daniel.arumi@upc.edu

Abstract: Non-volatile memory cells are exposed to adversary attacks since any active countermeasure is useless when the device is powered off. In this context, this work proposes the association of two serial RRAM devices as a basic cell to store sensitive data, which could solve this bothersome problem. This cell has three states: '1', '0', and masked. When the system is powered off or the data is not used, the cell is set to the masked state, where the cell still stores a '1' or a '0' but a malicious adversary is not capable of extracting the stored value using reverse engineering techniques. Before reading, the cell needs to be unmasked and it is masked afterwards until the next reading request. The operation of the cell also provides robustness against side-channel attacks. The presented experimental results confirm the validity of the proposal.

Keywords: RRAM; secure non-volatile memories; variability; masking; hardware security



Citation: Yang, B.; Arumí, D.; Manich, S.; Gómez-Pau, Á.; Rodríguez-Montañés, R.; González, M.B.; Campabadal, F.; Fang, L. Serial RRAM Cell for Secure Bit Concealing. *Electronics* **2021**, *10*, 1842. <https://doi.org/10.3390/electronics10151842>

Academic Editor: Dongseok Suh

Received: 4 June 2021

Accepted: 25 July 2021

Published: 31 July 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

In the IoT era, the ubiquitous use of sensitive and private data requires reliable and secure embedded systems where a reasonable amount of memory is required for security code encryption or key storage. This sensitive data is commonly stored in embedded non-volatile memories (NVMs) such as ROM, e-fuse (electronic-fuse) or anti-fuse, battery-backed SRAMs or logic EEPROM/Flash. Masked ROM memories store keys during manufacturing. Therefore, a change in the key requires modifying the mask layout. E-fuse [1] and anti-fuse [2,3] are one-time programmable (OTP) memories, which can be built in a generic digital process, but the programming operation is irreversible. A battery-backed SRAM is a power-gated SRAM in data retention mode. The battery is required to avoid the volatility of SRAM memories, at the expense of an increase in cost, complexity, and power consumption. Logic EEPROM/Flash [4–6] are based on the floating gate technology and have been successfully deployed in automotive microcontroller units (MCU) and smartcard ICs. However, they are still expensive and require additional masks and process steps in comparison with the standard CMOS technology. All these NVMs present the same security vulnerability, since data remain in the memory even without power, exposing it to potential attackers. Confidentiality attacks aim at extracting this stored information. In the case of NVMs, attackers aiming at stealing private data can succeed in their objective with the aid of cold-boot attacks or other removal strategies like stealing memory modules [7,8]. As an alternative, secret keys can also be extracted from security primitives, the so-called physical unclonable functions (PUFs) [9]. PUFs are physical structures that embrace manufacturing variations resulting from the IC fabrication process to generate a key. Although PUFs

provide a promising alternative for a key generation [10], they still pose challenges like low reliability, need for error detection and area overhead.

In this context, resistive random access memories (RRAMs) have emerged as a promising alternative to replace current memories [11,12]. Moreover, the inherent variability of RRAMs, due to the stochastic nature of their switching mechanism [13], has positioned these devices as one of the most competitive candidates for the development of security primitives [14]. In fact, RRAMs have attracted the attention of the research community for the implementation of PUFs [15–23] and true random number generators (TRNGs) [24–29]. Nevertheless, RRAM-based circuits may also introduce security vulnerabilities of their own. One of the main concerns is related to its inherent non-volatility, since data written to the memory persist even when the system is powered off, arising a similar problem as present NVMs. This fact may expose RRAMs to a variety of physical attacks, compromising data confidentiality [30]. For this reason, extensive effort is currently devoted to improving the security of RRAM-based memories. These approaches propose security improvements at the physical or circuit level [31–34] and at the authentication or encryption level [35,36]. However, all these proposed approaches still do not address the fundamental problem of privacy data remaining in memory after the power is turned off.

The present paper proposes the association of two RRAMs in a serial configuration as a basic cell for secure NVMs, which could solve this critical problem. This cell has already been proposed for other security applications [25,37,38]. However, unlike these previous works, in this paper the cell is excited in such a way that the deterministic switch of one of the RRAMs is obtained. The configurations of the cell where both devices are in different resistance states are leveraged to store one bit of information. The operation of the cell provides also the capability of masking and unmasking the data on demand. With this countermeasure the protection against physical attacks is enhanced when the device is powered off or when the sensitive data is not used. Furthermore, side-channel attacks that conduct information stealing by monitoring the current consumption are preventable in this work. The presented experimental results are a proof of concept that validates the applicability of the proposed cell. Moreover, a potential array architecture based on the serial RRAMs memory cell is proposed and its ability to defend the physical attacks is discussed.

The rest of the work is organized as follows. A short review about the use of RRAM devices as memory cells and related security aspects is found in Section 2. The serial RRAM memory cell and its functionality details are presented in Section 3. Next, experimental results are summarized in Section 4. An array architecture proposal based on the serial RRAM cell is found in Section 5. The security features arising from the cell and the proposed array architecture are discussed in Section 6. Finally, the conclusions are drawn in Section 7.

2. RRAM Cell and Security Aspects

RRAMs are devices belonging to the memristor type [39] and are typically composed of an electrode/dielectric/electrode stack structure. Its resistive switching mechanism relies on the formation and rupture of conductive filament (CF) based on defects in the oxide (dielectric) between the two metal electrodes [11]. For a RRAM in a pristine state an initial operation, called the forming process, is usually required to generate the CF. Once the CF is formed, a RRAM can reversibly switch between a high resistance state (HRS) and a low resistance state (LRS). This switching behavior is obtained by applying voltage pulses between the electrodes in a bipolar mode for most of the existing technologies [40]. Furthermore, when the voltage is removed, RRAM would memorize the current resistance state until the next voltage is applied and the resistance state can be maintained for several days or even years [41]. The switching operation from HRS to LRS is called the SET process, whereas the switching operation from LRS to HRS is called the RESET process. The non-volatility properties of RRAMs have motivated their use as memory devices, although

other fields such as digital logic, analog circuits, neural networks, and hardware security are also receiving considerable attention.

Concerning memory applications, there are mainly two array architectures for RRAM integration [42]: 1T1R and cross-point array. The former offers better write/read margins and has a bigger array size whereas the latter shows smaller cell area and lower power consumption. Furthermore, cross-point arrays typically include selectors (one-selector and one-resistor (1S1R) architecture) to prevent interference between cells and avoid the sneak-path issue. Figure 1a shows the typical scheme for the 1T1R array. The RRAM is in series with a cell selection transistor, which isolates the selected cell from other unselected cells. The word line (WL) controls the gate of the transistor. Therefore, tuning the WL voltage allows the control of the write current that is delivered to the cell. In Figure 1b, a crossbar array based on a 1S1R cell is shown. Each RRAM is connected at the cross-point between a word-line and a bit-line. A selector (two anti-parallel diodes-like device) is connected in series in order to minimize the sneak current effect. By applying positive or negative writing voltages to lines WL and BL, each RRAM can be switched to *HRS* or *LRS* thus storing a '1' or '0' bit.

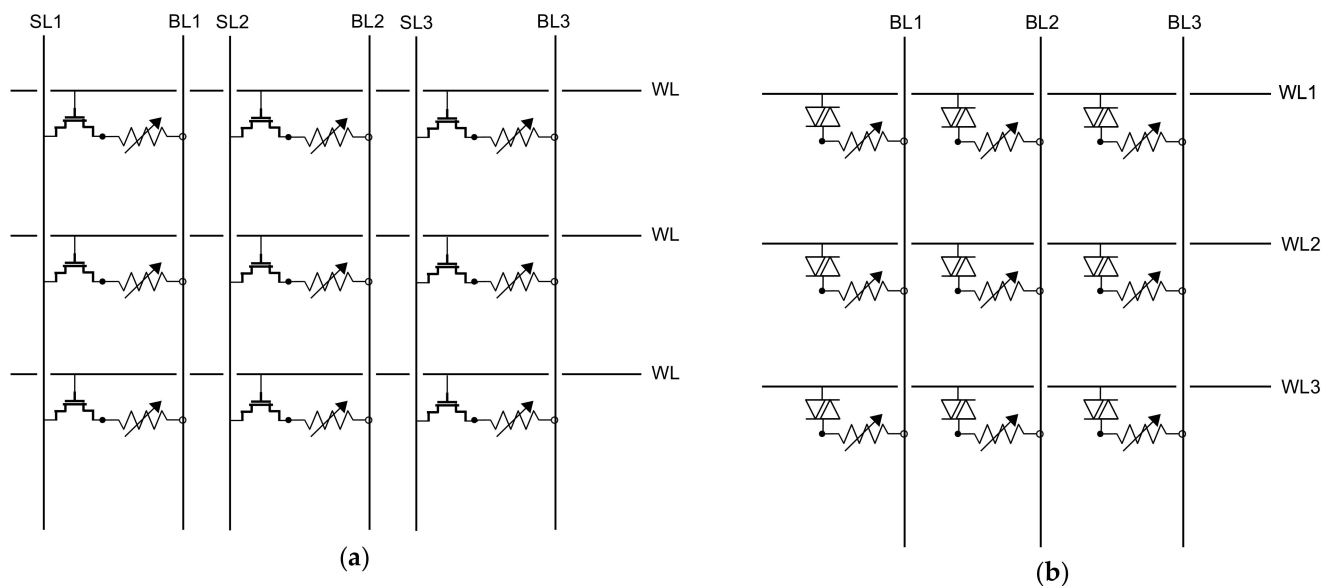


Figure 1. Array architectures for RRAM integration (a) 1T1R (b) 1S1R.

Memories storing sensitive information are usually protected by encrypting their content. However, for certain setups, keys need to be written in plaintext. A practical case can be seen in the Lohrke et al. paper for a real *Xilinx-FPGA* [43]. It becomes, then, important to have memories that are secure at the hardware level, in which the bits become self-protected against possible adversary attacks.

The RRAM-based technology is compatible with CMOS fabrication and is added at a backend process module. RRAMs layers are placed in the most external part of the chip in which the cross-point structures can be found [44]. From this, one immediate vulnerability can be identified by adversaries, who are able to apply reverse engineering techniques. As it is shown in Figure 2a, FIB equipment can be used to open access at row and column metal lines and to pin probes. From these, RRAM resistances can then be passively measured and bits are extracted. In Figure 2b a drawing illustrating this attack is shown and in Figure 2c it can be seen how probes can be pinned. Usually, the probes themselves cannot contact the lower layers through the opens but metallizations are added which bring the connections to the surface. This type of attack is usually prevented by adding protecting shields (active or passive). Anyhow, these shields are expensive and consume, at least, a full metallization layer [45].

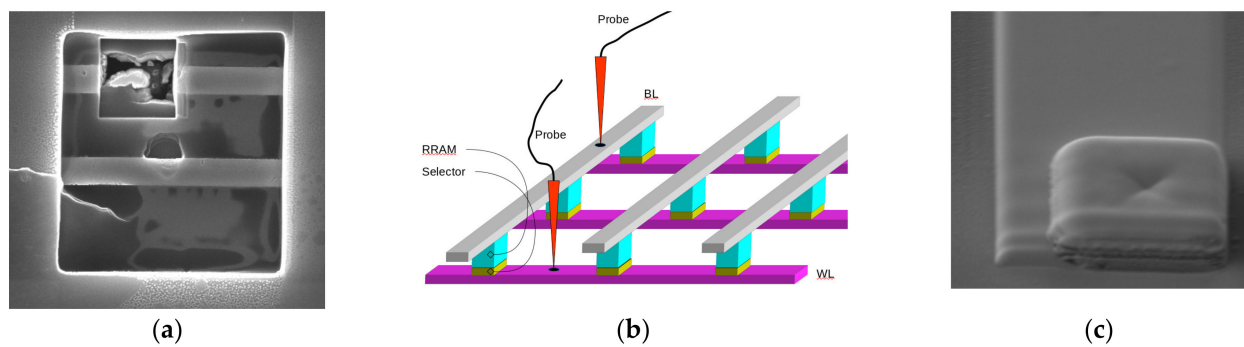


Figure 2. (a) Silicon edition with a $6 \times 6 \mu\text{m}^2$ open is made on the passivation layer to access the metal routing layers in a 65 nm CMOS technology chip. The inset open shows a lower connection via. (b) With direct contact probes, RRAM resistances can be passively measured using reverse engineering techniques. (c) After the FIB edition, extra deposition of metallic layers export connections below to the surface in order to ease the contact with probes. Pictures are from a hacked 65 nm chip reverse-engineered in CRnE-UPC-BarcelonaTech. The chip itself does not contain RRAMs but it illustrates the power of the FIB edition.

A second vulnerability exists during the reading of the cells. When a word line is activated, a set of RRAMs are biased with the reading voltage and the flowing current is sensed. The accumulated current becomes an image of the number of 1s and 0s that exist at this particular word, becoming correlated to the hamming weight. This kind of leakage is usually exploited by adversaries to revert keys from security chips using side-channel attack techniques. In this context, the improvement of security features of RRAM-based memories has become a topic of extensive research.

3. Serial RRAM Cell for Secure NVMs

The considered serial RRAM memory cell is a kind of differential cell in which bits can be concealed. As shown in Figure 3, it consists of two RRAMs connected in series. Four different cell states can be identified from the two possible resistance states of each RRAM, see Figure 4: $(HRS, LRS) \rightarrow '0'$, $(LRS, HRS) \rightarrow '1'$, $(LRS, LRS) \rightarrow \text{MASKED}$ in the LRS, $(HRS, HRS) \rightarrow \text{MASKED}$ in the HRS (NOT USED). The behavior of the cell is as follows: with the two RRAMs initially in the LRS, during a serial RESET (SRESET), i.e., a RESET operation of the two serially connected devices, one of the RRAMs switches to the HRS first. When the SRESET is initiated, the voltage across the switching device increases, preventing the other device to switch. During a subsequent serial SET (SSET), i.e., a SET operation of the two serially connected devices, only the RRAM in the HRS switches back to the LRS, since the other one is already in the LRS. For subsequent SSET and SRESET the switching device is always the same. The basic operation of the cell is reported in Figure 5. Furthermore, considering the unused configuration in which both RRAMs are masked in the HRS, one of the RRAMs switches first to the LRS in the subsequent SSET operation, which raises the voltage across the other non-switching RRAM device, forcing it to switch to the LRS as well. In this case, both devices may end up in the LRS if the SSET voltage is not withdrawn in time, compromising the functionality of the cell. That is the main reason why this configuration (HRS, HRS) is not adopted here. Given a particular pair of devices initially in the LRS, by applying consecutive SRESET and SSET operations the bit can be unmasked and masked, respectively. Depending on which of the RRAMs switches to the HRS after a SRESET, two different states of the cell can be differentiated (the so-called '0' or '1'). The RRAM that goes first to the HRS depends on device-to-device variability. Therefore, every cell generates an unpredictable bit, which is maintained during subsequent SRESET and SSET operations. Furthermore, it adds masking capability since both devices remain in the LRS after a SSET. This fact can be exploited to generate unpredictable bits with the potential application in PUFs [38].

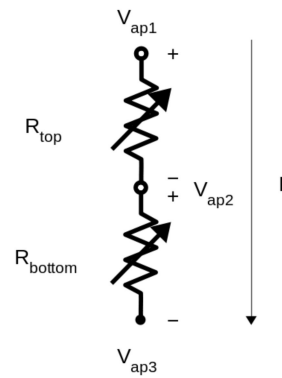


Figure 3. Serial RRAM cell for secure memory design.

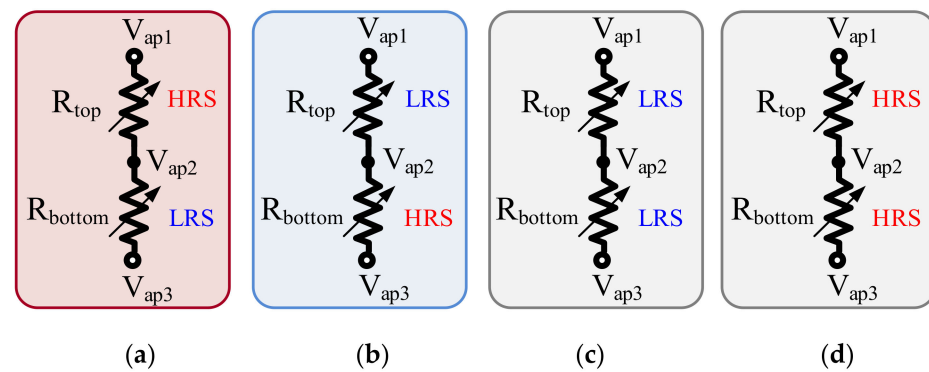


Figure 4. Data stored in the serial cell depends on the resistance state of the RRAMs: (a) ‘0’; (b) ‘1’; (c) Masked in the LRS; (d) Masked in the HRS.

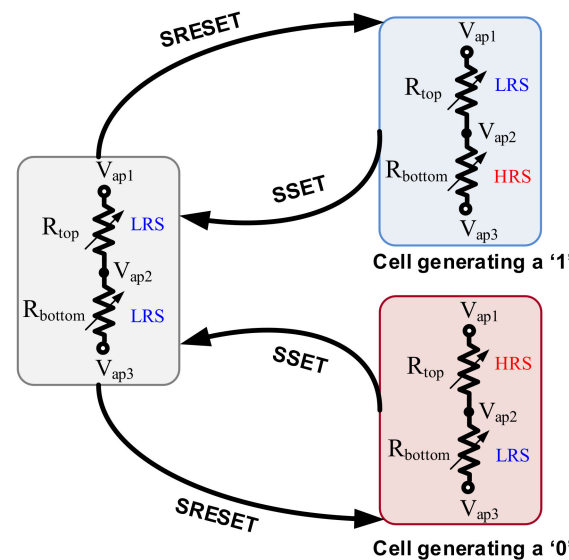


Figure 5. The basic operation of the serial RRAM cell for the generation of unpredictable bits.

This serial RRAM cell is proposed in the present work for secure NVMs. However, for this application, we must include writing capabilities to obtain a full operational memory cell. This fact requires the capability of writing data to the cell while maintaining the feature of masking/unmasking the bit. For this purpose, during the write operation, individual SET and RESET operations are applied so that the middle node V_{ap2} is grounded and nodes V_{ap1} and V_{ap3} are biased accordingly, as illustrated in Figure 6a,b for write-0 and write-1 operations, respectively. During masking and unmasking operations the middle node V_{ap2}

is left floating and voltages at nodes V_{ap1} and V_{ap3} are applied accordingly. The masking operation is performed by bringing the two RRAMs to *LRS* with a SSET, which forces the same current passing through both devices, see Figure 6c,d. After this operation, it is arduous to know what the previous combination of states (*HRS*, *LRS*) or (*LRS*, *HRS*) was. However, if an unmasking operation (SRESET) is applied (forcing the same current through both devices) the previous state (*HRS*, *LRS*) or (*LRS*, *HRS*) is restored, see Figure 6e,f. With the cell in an unmasked state, a read operation (SREAD) is conducted, as illustrated in Figure 6g,h. Node V_{ap3} is grounded and the read voltage is applied to node V_{ap1} while the voltage at the floating node V_{ap2} is measured and compared to a reference voltage to read the bit. The complete behavior of the cell is demonstrated next.

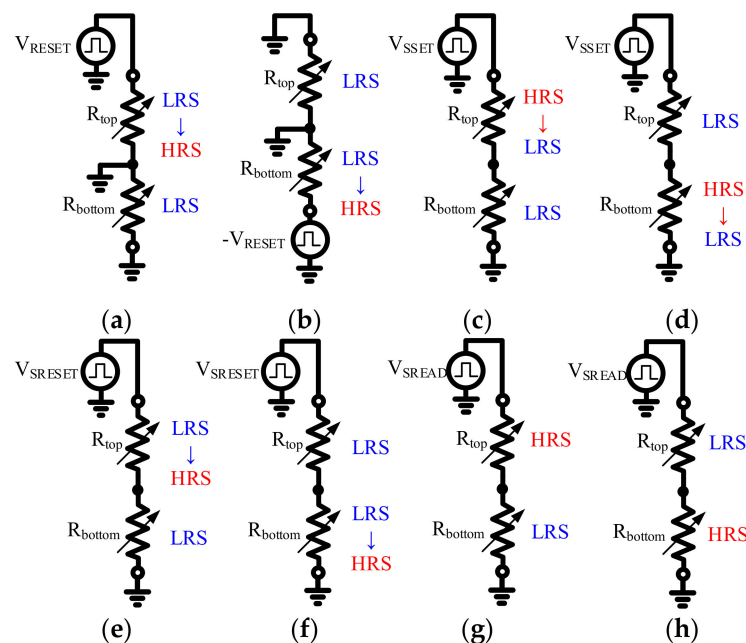


Figure 6. Configuration for the different cell operations: (a) write-0; (b) write-1; (c) masking ('0'); (d) masking ('1'); (e) unmasking ('0'); (f) unmasking ('1'); (g) serial read ('0'); (h) serial read ('1').

According to the different configurations of the cell reported in Figure 6, a full operation of the cell can be derived, as the sequence of operations illustrated in Figure 7. Starting from both devices in the *LRS*, a write operation is applied to the cell to store the secret bit (write-0 in Figure 7a and write-1 in Figure 7b). Subsequently, a masking operation is applied to conceal the bit. Then, the secret can be revealed on demand by applying an unmasking operation followed by a read operation. Once the information has been obtained, the secret is masked again. This sequence of operations (unmasking-read-masking) can be applied as many times as needed. In this way, the information is only exposed in a small fraction of time when it is used, remaining secured during the rest of the time, even when the system is powered off.

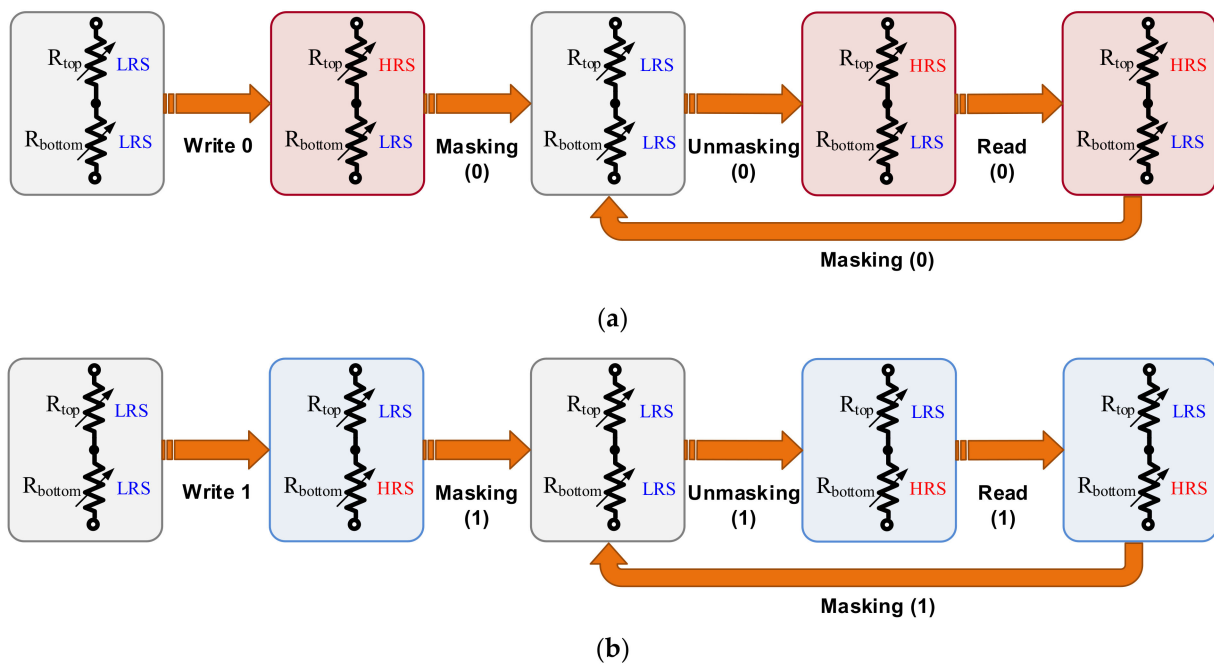


Figure 7. The sequence of operations and resistance state of the devices for the secure memory cell: (a) Initially writing '0'; (b) Initially writing '1'.

4. Experimental Results

Experiments were conducted to assess the feasibility of the proposed cell. The RRAM devices used in the experiments are TiN/Ti/HfO₂/W structures [20,38]. Figure 8a shows a schematic cross-section of the final device structure. A top view optical microscope image of the structures is illustrated in Figure 8b, which are square cells of 60 × 60 μm², 15 × 15 μm² and 5 × 5 μm². The electrical characterization of the devices was performed using two synchronized B2912A precision source/measure units (SMUs, Keysight, Santa Rosa, CA, USA). The typical resistive switching characteristics under DC conditions are shown in Figure 9a, where double-sweep voltage ramps were applied from 0 V to +1.1 V for the SET, and from 0 V to −1.4 V for the RESET operations. The corresponding cycling behavior under the pulse mode, using the same voltage amplitudes as those in DC conditions, is presented in Figure 9b.

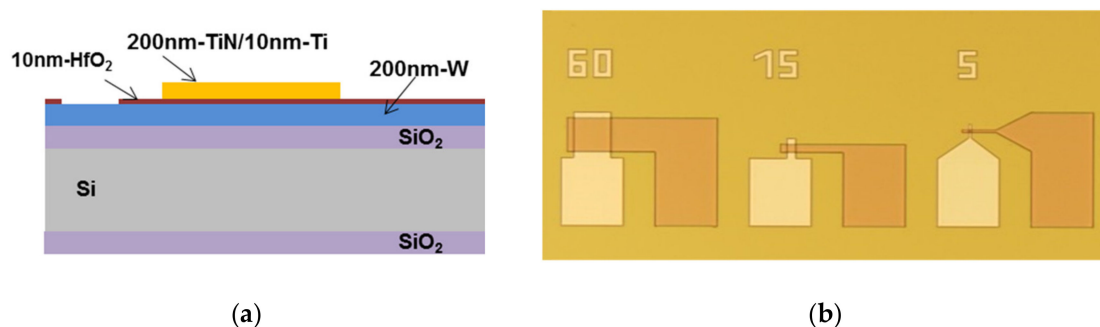


Figure 8. (a) Schematic device cross-section; (b) Top view optical microscope image of the fabricated devices.

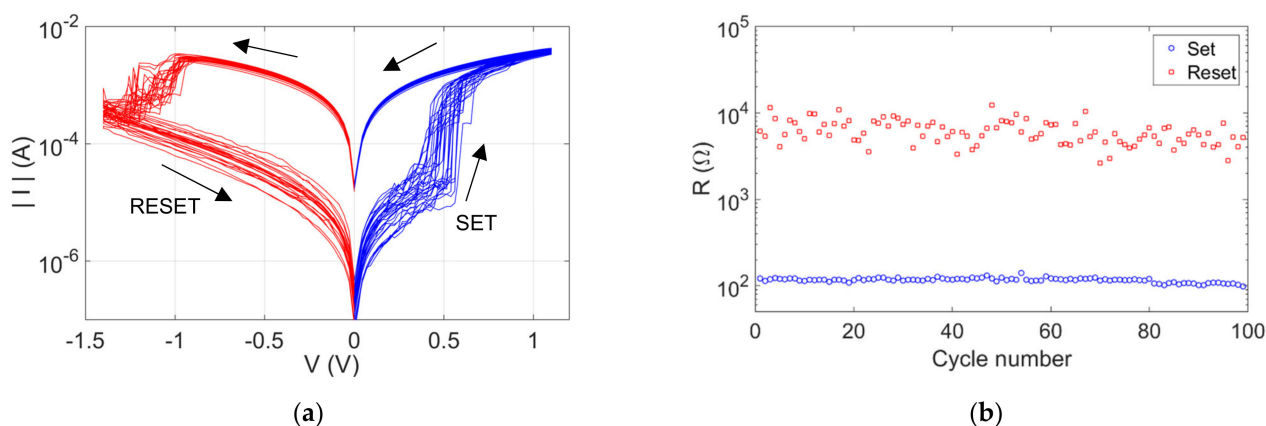


Figure 9. (a) DC resistive switching behavior during successive SET and RESET operations; (b) Resistances during pulsed SET and RESET operations.

The pulse mode was assessed and before checking the functionality as a memory cell, an initial experiment was performed to reproduce the results in [38]. It consisted in starting from both devices in the LRS, applying a sequence of unmasking–masking operations (both followed by a read operation) without forcing a write operation in advance, as illustrated in Figure 10. Which of the devices is going to switch after the first unmasking operation is unpredictable, but for subsequent masking/unmasking operations, the switching device is expected to be the same. Depending on which of the RRAMs switches to the HRS two different states of the cell ('0' or '1') can be differentiated, as previously presented in Figure 4a,b. Experimental results for a serial cell are shown in Figure 11a,b, which were derived from the read operations after masking and unmasking, respectively. In this example, R_{bottom} switches to the HRS, whereas R_{top} remains at the LRS. Considering the results in Figure 11b, and according to the definitions in Figure 4, '1' was stored in this example. However, Figure 11a shows that the bit ('1' in this particular example) is masked after a SSET since both devices remain in the LRS. The RRAM that goes first to the HRS depends on the LRS resistance and the RESET voltage of the devices in every particular cell. This persistent behavior is mainly due to the higher inter-device variability as compared to the intra-device variability, as shown in Figure 12a for the RESET voltage (V_{RESET}) and in Figure 12b for the resistance in the LRS (R_{LRS}). The data was derived from 25 DC cycles of 15 different devices.

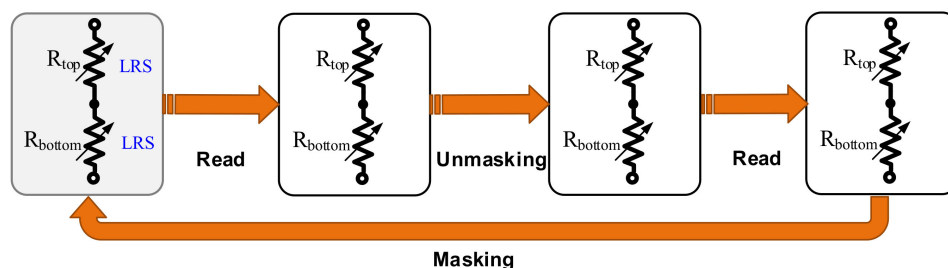


Figure 10. Diagram of operations and state transformation to reproduce the results in [38].

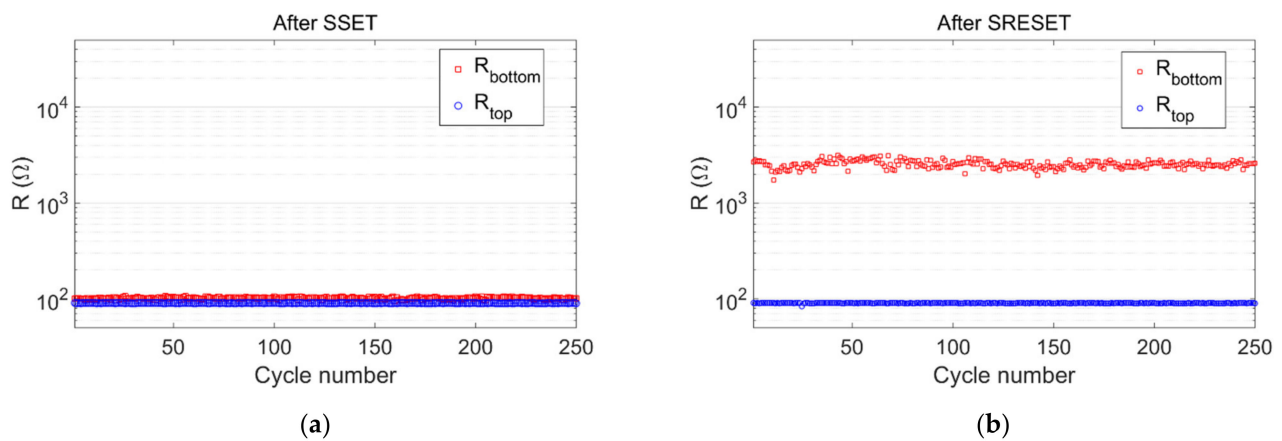


Figure 11. Measured resistances of a serial RRAM cell during a sequence of 250 serial operation cycles. No current compliance limit was imposed during SSET: (a) After masking (After SSET); (b) After unmasking (After SRESET).

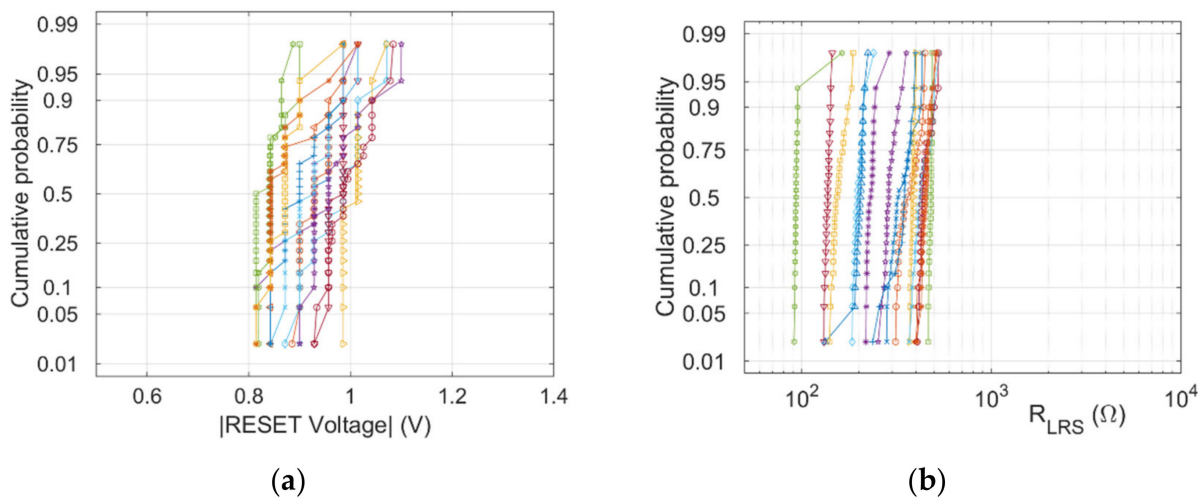


Figure 12. Cumulative probability obtained from 15 different single devices (color lines identify each device) corresponding to 25 DC cycles: (a) RESET voltage (V_{RESET}); (b) Resistance in the LRS (R_{LRS}).

The experimental set-up was subsequently upgraded in order to check the functionality of secure NVMs, including the ability to control which of the two RRAMs switches to the HRS. The corresponding results are presented in the next section.

Experiments were conducted on a set of RRAM pairs to validate the operation of the cell. The amplitude of the pulses applied during the experiments is summarized in Table 1. It must be taken into account that V_{SSET} and V_{SRESET} are slightly higher than the values corresponding to causing the SET and RESET of a single device, but they are low enough to avoid the degradation of the devices.

Table 1. Amplitudes of the voltage pulses used in the experiments.

Operation	Cell Configuration	Voltage (V)
Initialization to LRS	SET (V_{SET})	1.1
Write-0/Write-1	RESET (V_{RESET})	−1.4
Unmasking	Serial RESET (V_{SRESET})	−1.7
Masking	Serial SET (V_{SSET})	1.6
Read	Serial read (V_{SREAD})	0.2

The first experiment was devoted to checking the ability to unmask and mask the bit written in the cell. The sequence of operations was similar to the one shown in Figure 7.

The only difference is that we included an extra read operation to check the state of the cell after masking, which would not be required in normal operation mode. Hence, starting from both devices in the *LRS*, a write-0 operation was applied, followed by a sequence of 1000 unmasking-read-masking-read operations. The equivalent experiment was also conducted with an initial write-1 operation. The voltage measured at the common terminal of the two devices (V_{ap2}) during the SREAD operation is shown in Figure 13a,b after an unmasking and masking operation, respectively. It is observed that the stored bit can be unmasked and masked 1000 times. After unmasking, the measured voltage is close to 0 V when '0' was initially written to the cell. On the contrary, the measured voltage was close to 0.2 V (V_{SREAD}) when '1' was initially written in the cell. However, an intermediate voltage was measured after masking regardless of the initial written value. In fact, the two sets of voltage measurements are overlapped. Thus, it is unlikely to predict whether '0' or '1' is stored under the masked state.

The resistances of the devices derived from the results in Figure 13 are represented in Figure 14. After the unmasking operation (Figure 14a) both devices are in different resistance states, depending on which value was written to the cell in advance. However, once masked, both devices remain in the *LRS*. The resistance values are quite similar regardless of the value initially stored in the cell, as observed in Figure 14b. Therefore, these results demonstrate that we can deterministically determine the switching RRAM of the cell, i.e., writing the desired data to the cell (0 or 1), and we can subsequently mask and unmask the previous written data repeatedly.

Experiments were also conducted to check the behavior of the masked bit over time. In particular, the goal consisted in extending the masked state for 10^4 s, verifying throughout the experiment that it was stored (masked) successfully. The corresponding results showing the resistance values of the RRAMs are shown in Figure 15a,b when '0' was initially written to the cell. The equivalent values are presented in Figure 16a,b when '1' was initially written to the cell. The results confirm that the bit can be unmasked and masked for at least 10^4 s.

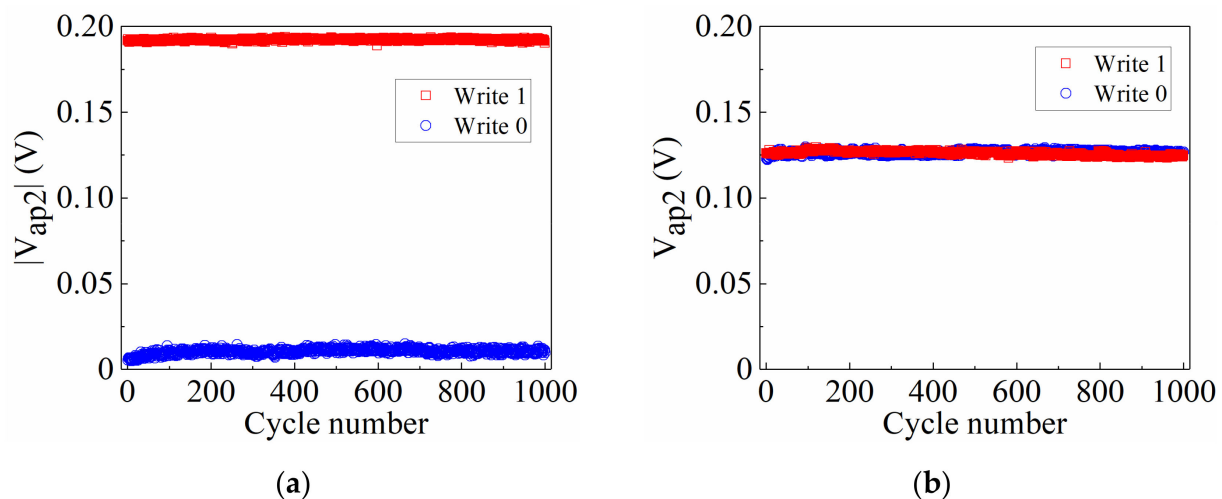


Figure 13. Measured voltage values at the common terminal of the two devices (V_{ap2}) during SREAD: (a) after unmasking; (b) after masking. The operations were repeated 1000 times after initially applying a write-1 and a write-0 operation.

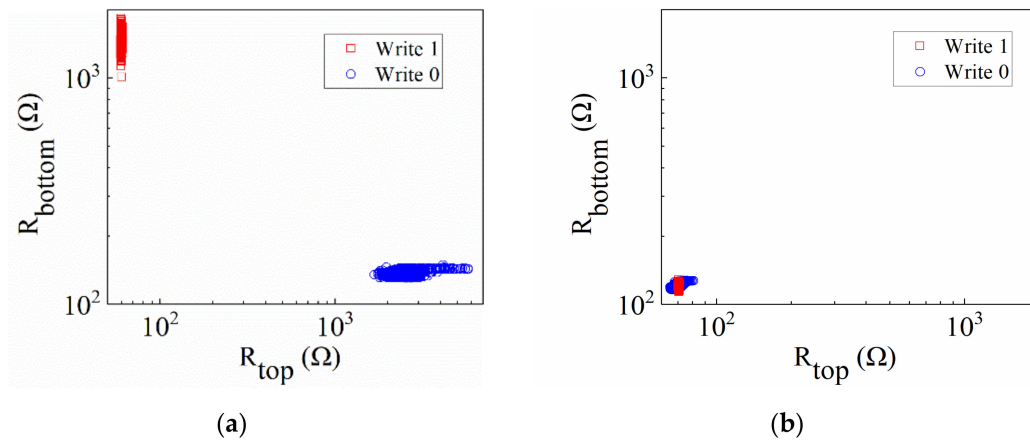


Figure 14. Resistance values of the RRAMs derived from the read operations during the sequence of 1000 unmasking-read-masking-read operations: (a) after unmasking; (b) after masking.

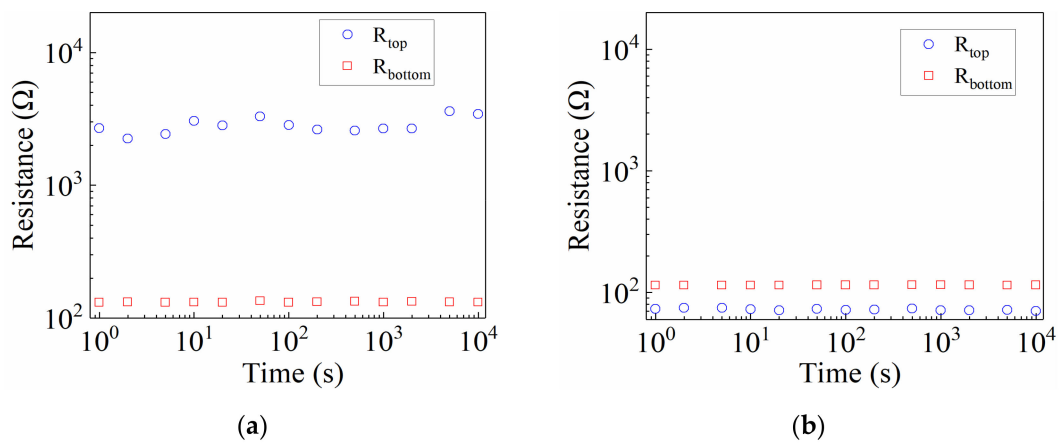


Figure 15. Resistance values of the RRAMs during unmasking-masking operation for 10^4 s. Initially, '0' was written to the cell: (a) after unmasking; (b) after masking.

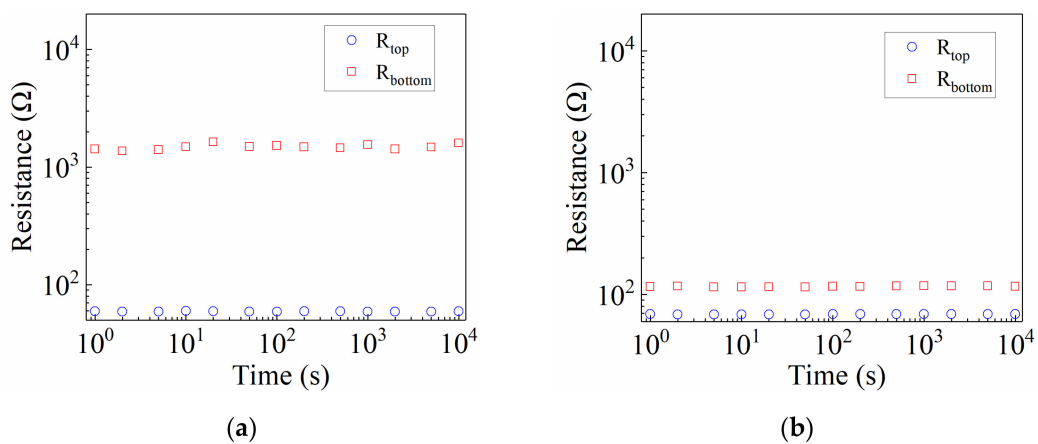


Figure 16. Resistance values of the RRAMs during unmasking-masking operation for 10^4 s. Initially, '1' was written to the cell: (a) after unmasking; (b) after masking.

The final experiment focused on observing the behavior of the cell in case we want to modify the bit stored in the cell. For this purpose, a sequence of 1000 write-masking-read-unmasking-read operations was applied, where the write operations (write-0 or write-1) were randomly selected. An illustrative example of the behavior of the cell is reported in

Figure 17. The resistances of the two devices are derived from the read operations after unmasking (Figure 17a) and masking (Figure 17b). The switching device is always the expected RRAM, according to the value written to the cell. Furthermore, the resistances in the *LRS* of the two RRAMs are very similar in the masked state regardless of the previous write operation. In fact, the two sets of points overlap, as observed in Figure 17b. This feature, which allows rewriting the cell many times, confirm the use of this cell as a memory cell. In fact, it can also be exploited for reconfiguration purposes or the removal of the information stored in the cell in those applications where the information is rarely updated. In fact, these results, together with the capability of masking and unmasking the data, confirm the suitability of this cell for application in secure NVMs.

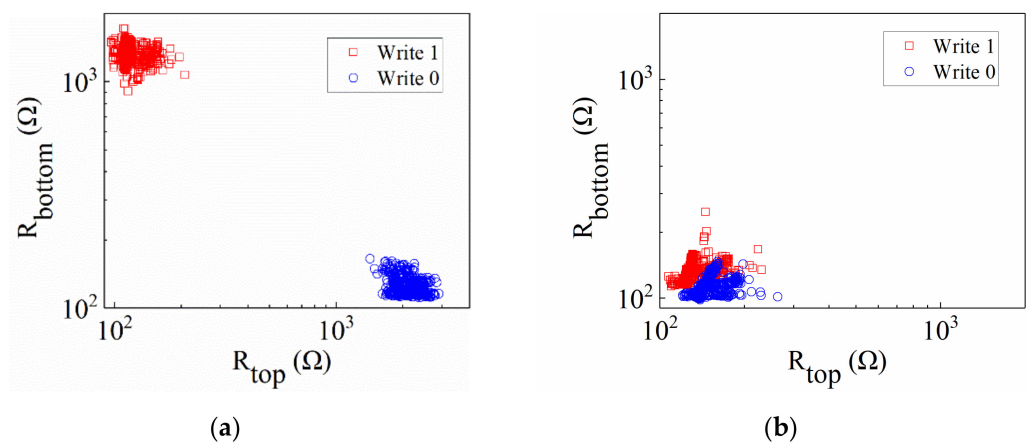


Figure 17. RRAM resistances of a serial cell during a sequence of 1000 write-unmasking-masking cycles with random Scheme 0. operation: (a) After unmasking; (b) After masking.

5. Array Architecture

The experimental results presented in the previous section demonstrate that the serial RRAM cell can be exploited to store one bit of information with masking capability. Hence, it is feasible to combine multiple cells into an array structure to derive a secure NVM. A cross-point array could be considered for this purpose. However, some design modifications are required to derive the serial RRAM cell, i.e., connecting the bottom electrode of the top device to the top electrode of the bottom device. This array meets the requirements from the operational point of view, but it also adds security vulnerabilities in the presence of a physical attack. In fact, as all the devices are in the same layer, this configuration exposes node V_{ap2} (see Figure 3) so that an attacker may contact this node without destroying the cell structure, with the potential risk of leak of information. In this context, we propose a multilayer array architecture, as illustrated in Figure 18. Multilayer RRAMs is a technology that has been already proposed as a way for building denser memories [44–46], therefore it can also be leveraged for this serial RRAM cell configuration, avoiding the need of a specific array design or technology, which could discourage its implementation. Two word-lines are necessary to bias nodes V_{ap1} (WL1) and V_{ap3} (WL2) while nodes V_{ap2} are connected through transmission gates to the bit lines. As it is indicated in Figure 18a, for reading the cells in one word-line, WL2 is grounded and the reading voltage is applied to WL1. Transmission gates are enabled and voltages at BLs are compared for extracting the bit information. Typically, the reading process is made by word lines steps. Initially, the cells in one word line are unmasked, read and masked again before moving to the next word line. In this way, most of the cells remain masked during most of the time. Although every cell is composed of two devices, the proposed architecture provides similar performance in terms of scalability when compared to other RRAM security primitives, which consider differential sensing, requiring thus also two devices to derive a single bit. Figure 18b shows a 3D illustration of the memory array. Two layers of RRAMs are used. The lower layer contains the bottom RRAMs whereas the upper layer contains

the top RRAMs. The lower layer (labeled as the shadow in Figure 18a) is placed so that their geometric position coincides with the upper layer. This gives them a natural sheet protection against physical attacks as it is discussed next.

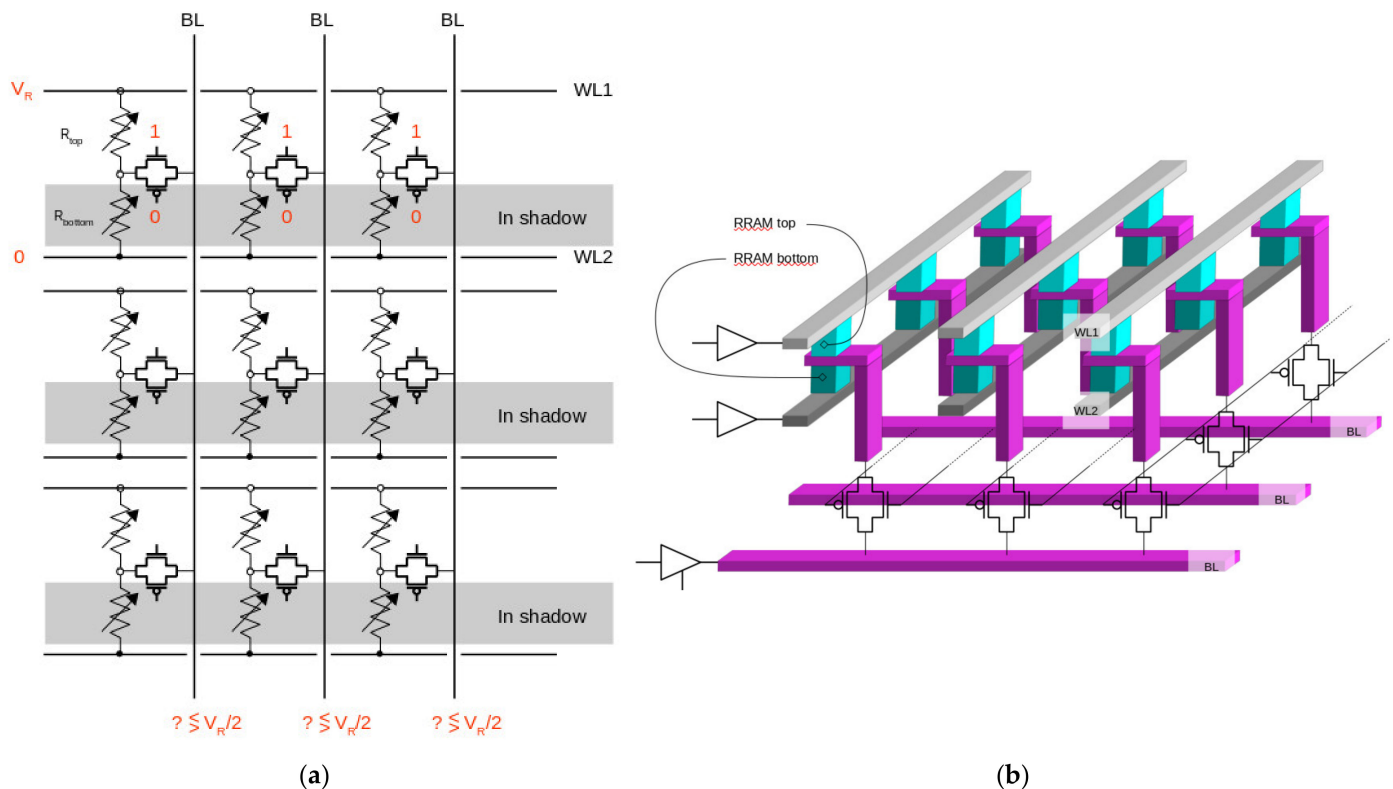


Figure 18. Serial RRAM memory array. (a) Schematic distribution of elements. RRAMs (R_{bottom}) in the shadow area are built under R_{top} RRAMs, so that they become shielded (protected) against physical attacks. (b) A 3D view of the structure.

6. Security Features

The memory array based on a serial RRAM cell presents advantages against physical and side-channel attacks. In the case of physical attacks, it is plausible to assume that the adversary cannot read the content of on-chip resources nor the data bus since on-chip components are trustworthy (data protection techniques at a higher level are assumed to be active in the system) during its operation. However, off-chip components, such as the memory modules, or on-chip elements while the chip is powered off, are assumed to be vulnerable since the attacker is considered to have physical access using reverse engineering techniques. In this situation, a potential memory array based on serial RRAM cells embraces the same security performance against physical attacks as other RRAM-based memories. Furthermore, as there is no charge stored in RRAMs, the states are not exposed by charge-detection-type attacks, as they may be in floating-gate-based EEPROM/Flash memories. An adversary may try to measure passively RRAM resistances to reveal the state of the cell and therefore the stored bit. However, both RRAMs of the same cell are at the LRS in the masked state. Thus, reading the top device is not enough to get the information. The attacker would need also to measure the bottom one and then apply some types of reasoning trying to envisage the unmasked bit. Accessing the bottom RRAM is not easy and definitively makes the attack considerably complicated. As shown in Figure 19, using FIB edition a vertical cut must be opened which would break WL1 and thus would corrupt the operation of the memory array. If metallization depositions are made in order to restore the connection, easily they would become into a short circuit between WL1 and WL2 lines. An alternative to the passive measurement of resistances would be to contact the intermediate node V_{ap2} and try to detect the voltage during the read operation. Despite

not impossible, it is highly probable that the parasitic effects of the probe, which will be significant at this scale, will alter the unmasking process giving a wrong bit as a result. Even in a context where RRAM devices are reverse-engineering without destroying the storage structure, it would not be possible to differentiate between '0' and '1' by using high-resolution microscopy, since the two devices of every cell are in the LRS (masked state) as the attack is performed when the system is powered off. Therefore, despite not impossible, the difficulty to reach a successful physical attack in the serial RRAM memory array is expected to be much higher than that in the standard memory array.

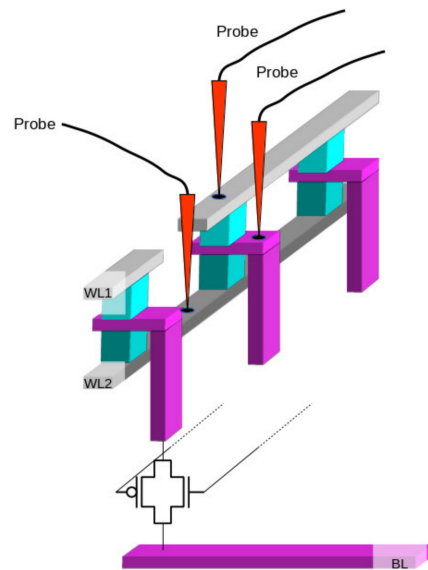


Figure 19. Measuring the two RRAM resistances of the serial cell requires access to line WL2 with a probe. In this configuration, it forces a cut in WL1 which will break the memory array functionality.

The side-channel attack is one of the most widely adopted methods to steal private data in the hardware security field, which exploits the different signatures in current information when reading/writing '1' and '0' bits. Therefore, one way to protect against the side-channel attack is trying to eliminate the difference in current information when operating with '1' and '0' bits. The proposed serial RRAM cell in this work achieved this point by causing the operation currents to be uncorrelated with the data stored in the cell. In the masking operation, it is always that one of the RRAM devices is in the HRS whereas the other one in the LRS no matter which bit is stored in the cell. In this case, the current information for any masking operation with '1' or '0' bit is relatively similar. The same analysis applies to the unmasking and read operations, in the former of which both RRAM devices of the cell are in the LRS regardless of which bit is stored in the cell whereas the latter faces the same distribution of RRAM resistance states as the masking operation. Hence, the current consumption of a given cell is dependent on the detailed resistance state of RRAM devices, but independent on the stored bit. The inherent cycle-to-cycle and device-to-device variability of RRAMs result in different current consumption behaviors among cells, preventing an unintended leakage of information. To illustrate this fact, the quiescent current consumption of a serial RRAM memory cell during masking, unmasking and read (after unmasking) operation for 1000 cycles is shown in Figure 20a–c, respectively. Both situations, initially applying a write-1 and a write-0 have been considered. Regardless of the value initially written to the cell, the current consumption is similar in every operation. Although the distributions are not completely overlapped, the extraction of information for a particular cell is not worthy to predict the behavior of the remaining cells, since every cell has its particular behavior depending on the inherent variability and stochasticity of the devices. This fact is shown in Figure 21,

where the quiescent current consumption during a read operation (after unmasking) is presented for two more cells, in a similar way as it has been presented in Figure 20c.

These memory cells refer to three different serial RRAM memory cells, each of which is composed of two RRAM devices in series. The three representative examples illustrate three different behaviors in terms of current consumption during read after unmasking operation. For cell 1 (Figure 20c), the current consumption is slightly higher when a '0' has been written to the cell. On the contrary, cell 2 (Figure 21a) presents higher current consumption when a '1' has been written to the cell and cell 3 (Figure 21b) presents an almost completely overlapping between the two distributions, becoming more similar to the behavior of cell 1. Therefore, the serial RRAM cell does not present distinguishable current signatures, which may minimize the possibility of information leakage.

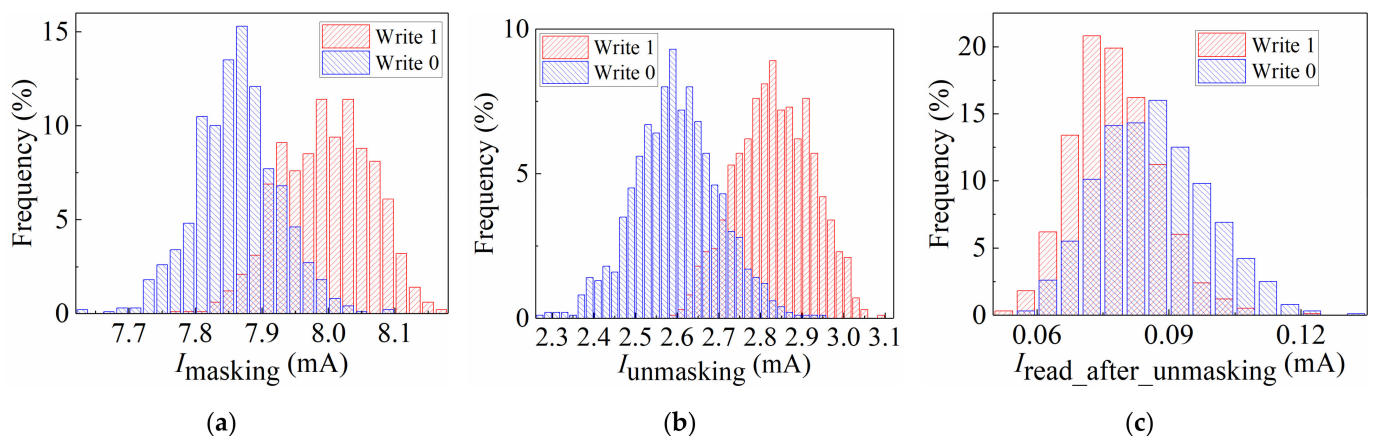


Figure 20. Quiescent Current histogram of cell 1 for 1000 cycles during: (a) Masking; (b) Unmasking; (c) Read after unmasking.

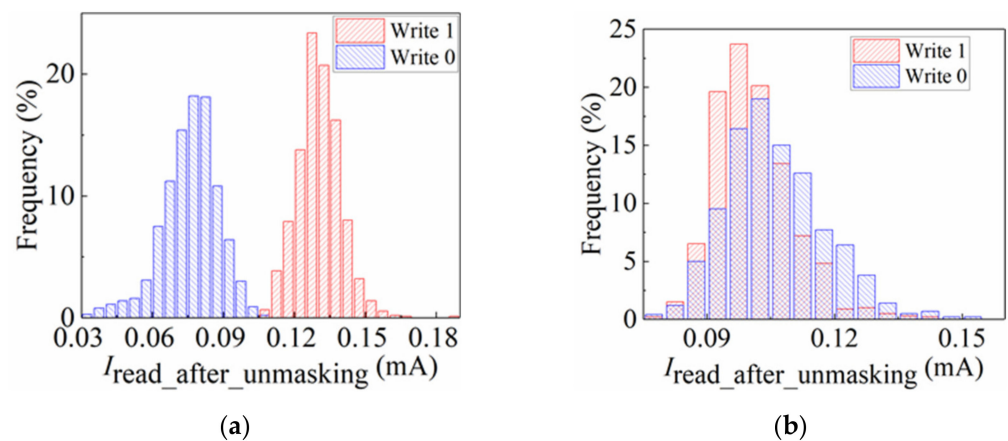


Figure 21. Quiescent current histogram for 1000 read operations (after unmasking): (a) cell 2; (b) cell 3.

The serial cell provides also the feature of rewriting the content, maintaining the masking capability, as it has been previously shown in Figure 17. This fact paves the way for memory reconfiguration, which can be utilized to update the information or for fresh re-keying [47,48]. When the original key has been revealed or the ownership is revoked and the user needs a new key, this scheme is useful, which can also limit the side-channel exposure of per-key. In fact, the same scheme can be also used for shredding when the key is no longer needed. In any case, it must be taken into account that a memory array based on the serial RRAM cell can be combined with other existing security features, at different levels, to improve the security performance of the resulting primitive.

7. Conclusions

The present work proposes the novel use of the serial configuration of two RRAMs as a memory cell with the extra capability of data masking. This serial cell presents three states: '1', '0' and masked. In the masked state, both RRAMs remain in the LRS, improving the data protection against physical attacks when the device is powered off. Furthermore, the symmetry of the cell's operation complicates the information stealing by monitoring the current consumption of the cells. Experimental work has been conducted on RRAMs devices where the functionality of the serial cell is confirmed. Moreover, it is demonstrated that this cell provides the permission of rewriting or updating its content, which can be useful for reconfiguration purposes. These experimental results are a proof of concept that demonstrates the applicability of this design for secure NVMs. An array configuration has also been proposed based on the serial RRAM cell, which can be leveraged to derive a secure NVM. It has been shown how this array self-shields each cell against reverse engineering techniques and provides robustness against side-channel attacks, which paves the way to the application of RRAMs for secure NVMs. However, a physical implementation of the proposed serial RRAM cell array was not achieved, as well as the security performance experiment with all the existing attacking methods, both of which are expected in our future work.

Author Contributions: Conceptualization, D.A. and S.M.; methodology, B.Y., D.A., S.M. and R.R.-M.; software, B.Y. and D.A.; validation, B.Y., D.A. and S.M.; formal analysis, B.Y., D.A., Á.G.-P. and L.F.; investigation, B.Y. and D.A.; resources, R.R.-M., M.B.G. and F.C.; writing—original draft preparation, B.Y., D.A. and S.M.; writing—review and editing, R.R.-M., Á.G.-P., M.B.G., F.C. and L.F.; funding acquisition, R.R.-M. and F.C. All authors have read and agreed to the published version of the manuscript.

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

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Shi, M.; He, J.; Zhang, L.; Ma, C.; Zhou, X.; Lou, H.; Zhuang, H.; Wang, R.; Li, Y.; Ma, Y.; et al. Zero-mask contact fuse for one-time-programmable memory in standard CMOS processes. *IEEE Electron. Device Lett.* **2011**, *32*, 955–957. [[CrossRef](#)]
2. Peng, J.; Rosendale, G.; Fliesler, M.; Fong, D.; Wang, J.; Ng, C.; Liu, Z.S.; Luan, H. A novel embedded OTP NVM using standard foundry CMOS logic technology. In Proceedings of the 2006 21st IEEE Non-Volatile Semiconductor Memory Workshop, Monterey, CA, USA, 12–16 February 2006; IEEE: Monterey, CA, USA, 2006; pp. 24–26. [[CrossRef](#)]
3. Chou, S.Y.; Chen, Y.S.; Chang, J.H.; Chih, Y.D.; Chang, T.Y.J. 11.3 A 10 nm 32 Kb low-voltage logic-compatible anti-fuse one-time-programmable memory with anti-tampering sensing scheme. In Proceedings of the 2017 IEEE International Solid-State Circuits Conference (ISSCC), San Francisco, CA, USA, 5–9 February 2017; IEEE: San Francisco, CA, USA, 2017; pp. 200–201. [[CrossRef](#)]
4. Raszka, J.; Advani, M.; Tiwari, V.; Varisco, L.; Hacobian, N.D.; Mittal, A.; Han, M.; Shirdel, A.; Shubat, A. Embedded flash memory for security applications in a 0.13/ μm CMOS logic process. In Proceedings of the 2004 IEEE International Solid-State Circuits Conference (IEEE Cat. No. 04CH37519), San Francisco, CA, USA, 15–19 February 2014; IEEE: San Francisco, CA, USA, 2014; pp. 46–512. [[CrossRef](#)]
5. Lee, Y.K.; Moon, J.H.; Kim, Y.H.; Chun, M.J.; Ha, S.Y.; Choi, S.; Yoo, H.; Jeon, H.; Yu, J.; Han, J.U.; et al. 2T-FN eNVM with 90 nm logic process for smart card. In Proceedings of the 2008 Joint Non-Volatile Semiconductor Memory Workshop and International Conference on Memory Technology and Design, Opio, France, 18–22 May 2008; IEEE: Opio, France, 2008; pp. 26–27. [[CrossRef](#)]
6. Hidaka, H. Evolution of embedded flash memory technology for MCU. In Proceedings of the 2011 IEEE International Conference on IC Design & Technology, Kaohsiung, Taiwan, 2–4 May 2011; IEEE: Kaohsiung, Taiwan, 2011; pp. 1–4. [[CrossRef](#)]
7. Halderman, J.A.; Schoen, S.D.; Heningner, N.; Clarkson, W.; Paul, W.; Calandrino, J.A.; Feldman, A.J.; Appelbaum, J.; Felten, E.W. Lest we remember: Cold-boot attacks on encryption keys. *Commun. ACM* **2009**, *52*, 91–98. [[CrossRef](#)]
8. Young, V.; Nair, P.J.; Qureshi, M.K. DEUCE: Write-efficient encryption for non-volatile memories. *ACM SIGARCH Comput. Archit. News* **2015**, *43*, 33–44. [[CrossRef](#)]
9. Herder, C.; Yu, M.D.; Koushanfar, F.; Devadas, S. Physical unclonable functions and applications: A tutorial. *Proc. IEEE* **2014**, *102*, 1126–1141. [[CrossRef](#)]

10. Sigl, G.; Gross, M.; Pehl, M. Where technology meets security: Key storage and data separation for system-on-chips. In Proceedings of the 2018-IEEE 44th European Solid State Circuits Conference (ESSCIRC), Dresden, Germany, 3–6 September 2018; IEEE: Dresden, Germany, 2018; pp. 12–17. [\[CrossRef\]](#)
11. Wong, H.S.P.; Lee, H.Y.; Yu, S.; Chen, Y.S.; Wu, Y.; Chen, P.S.; Lee, B.; Chen, F.T.; Tsai, M.J. Metal-oxide RRAM. *Proc. IEEE* **2012**, *100*, 1951–1970. [\[CrossRef\]](#)
12. Wu, H.; Wang, X.H.; Gao, B.; Deng, N.; Lu, Z.; Haukness, B.; Bronner, G.; Qian, H. Resistive random access memory for future information processing system. *Proc. IEEE* **2017**, *105*, 1770–1789. [\[CrossRef\]](#)
13. Yu, S.; Guan, X.; Wong, H.S.P. On the stochastic nature of resistive switching in metal oxide RRAM: Physical modeling, Monte Carlo simulation, and experimental characterization. In Proceedings of the 2011 International Electron Devices Meeting (IEDM), Washington, DC, USA, 5–7 December 2011; IEEE: Washington, DC, USA, 2011; pp. 17.3.1–17.3.4. [\[CrossRef\]](#)
14. Rajendran, J.; Karri, R.; Wendt, J.B.; Potkonjak, M.; McDonald, N.; Rose, G.S.; Wsocki, B. Nano meets security: Exploring nanoelectronic devices for security applications. *Proc. IEEE* **2015**, *103*, 829–849. [\[CrossRef\]](#)
15. Chen, A. Utilizing the Variability of Resistive Random Access Memory to Implement Reconfigurable Physical Unclonable Functions. *IEEE Electron. Device Lett.* **2015**, *36*, 138–140. [\[CrossRef\]](#)
16. Liu, R.; Wu, H.; Pang, Y.; Qian, H.; Yu, S. Experimental characterization of physical unclonable function based on 1 kb resistive random access memory arrays. *IEEE Electron. Device Lett.* **2015**, *36*, 1380–1383. [\[CrossRef\]](#)
17. Mazady, A.; Rahman, M.T.; Forte, D.; Anwar, M. Memristor PUF—A security primitive: Theory and experiment. *IEEE J. Emerg. Sel. Top. Circuits Syst.* **2015**, *5*, 222–229. [\[CrossRef\]](#)
18. Pang, Y.; Wu, H.; Gao, B.; Deng, N.; Wu, D.; Liu, R.; Yu, S.; Chen, A.; Qian, H. Optimization of RRAM-based physical unclonable function with a novel differential read-out method. *IEEE Electron Device Lett.* **2017**, *38*, 168–171. [\[CrossRef\]](#)
19. Uddin, M.; Majumder, M.B.; Rose, G.S. Robustness analysis of a memristive crossbar PUF against modeling attacks. *IEEE Trans. Nanotechnol.* **2017**, *16*, 396–405. [\[CrossRef\]](#)
20. Arumí, D.; Gómez-Pau, Á.; Manich, S.; Rodríguez-Montañés, R.; González, M.B.; Campabadal, F. Unpredictable bits generation based on RRAM parallel configuration. *IEEE Electron Device Lett.* **2018**, *40*, 341–344. [\[CrossRef\]](#)
21. Lee, G.S.; Kim, G.H.; Kwak, K.; Jeong, D.S.; Ju, H. Enhanced reconfigurable physical unclonable function based on stochastic nature of multilevel cell RRAM. *IEEE Trans. Electron Devices* **2019**, *66*, 1717–1721. [\[CrossRef\]](#)
22. Lin, B.; Gao, B.; Pang, Y.; Tang, J.; Qian, H.; Wu, H. A Unified Memory and Hardware Security Module Based on the Adjustable Switching Window of Resistive Memory. *IEEE J. Electron Devices Soc.* **2020**, *8*, 1257–1265. [\[CrossRef\]](#)
23. Zhao, Q.; Zheng, W.; Zhao, X.; Cao, Y.; Zhang, F.; Law, M.K. A $108 F^2$ /Bit Fully Reconfigurable RRAM PUF Based on Truly Random Dynamic Entropy of Jitter Noise. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2020**, *67*, 3866–3879. [\[CrossRef\]](#)
24. Huang, C.Y.; Shen, W.C.; Tseng, Y.H.; King, Y.C.; Lin, C.J. A contact-resistive random-access-memory-based true random number generator. *IEEE Electron Device Lett.* **2012**, *33*, 1108–1110. [\[CrossRef\]](#)
25. Balatti, S.; Ambrogio, S.; Carboni, R.; Milo, V.; Wang, Z.; Calderoni, A.; Ramaswamy, N.; Ielmini, D. Physical unbiased generation of random numbers with coupled resistive switching devices. *IEEE Trans. Electron Devices* **2016**, *63*, 2029–2035. [\[CrossRef\]](#)
26. Sahay, S.; Kumar, A.; Parmar, V.; Suri, M. OxRAM RNG circuits exploiting multiple undesirable nanoscale phenomena. *IEEE Trans. Nanotechnol.* **2017**, *16*, 560–566. [\[CrossRef\]](#)
27. Govindaraj, R.; Ghosh, S.; Katkooi, S. CSRO-based reconfigurable true random number generator using RRAM. *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.* **2018**, *26*, 2661–2670. [\[CrossRef\]](#)
28. Lin, B.; Gao, B.; Pang, Y.; Yao, P.; Wu, D.; He, H.; Tang, J.; Qian, H.; Wu, H. A high-speed and high-reliability TRNG based on analog RRAM for IoT security application. In Proceedings of the 2019 IEEE International Electron Devices Meeting (IEDM), San Francisco, CA, USA, 7–11 December 2019; IEEE: San Francisco, CA, USA, 2019; pp. 14.8.1–14.8.4. [\[CrossRef\]](#)
29. Aziza, H.; Postel-Pellerin, J.; Bazzi, H.; Canet, P.; Moreau, M.; Della Marca, V.; Harb, A. True random number generator integration in a resistive RAM memory array using input current limitation. *IEEE Trans. Nanotechnol.* **2020**, *19*, 214–222. [\[CrossRef\]](#)
30. Kannan, S.; Karimi, N.; Sinanoglu, O.; Karri, R. Security Vulnerabilities of Emerging Nonvolatile Main Memories and Countermeasures. *IEEE Trans. Comput. Aided Des. Integr. Circuits Syst.* **2015**, *34*, 2–15. [\[CrossRef\]](#)
31. Khedkar, G.; Kudithipudi, D.; Rose, G.S. Power profile obfuscation using nanoscale memristive devices to counter DPA attacks. *IEEE Trans. Nanotechnol.* **2014**, *14*, 26–35. [\[CrossRef\]](#)
32. Xie, Y.; Xue, X.; Yang, J.; Lin, Y.; Zou, Q.; Huang, R.; Wu, J. A logic resistive memory chip for embedded key storage with physical security. *IEEE Trans. Circuits Syst. II Express Briefs* **2015**, *63*, 336–340. [\[CrossRef\]](#)
33. Xiao, Y.; Xie, Y.; Yan, S.; Zhou, L.; Zhou, B.; Zhou, S.; Lin, Y. A physically-secure write scheme of Multi-time Programmable RRAM for critical information storage. In Proceedings of the 2016 13th IEEE International Conference on Solid-State and Integrated Circuit Technology (ICSICT), Hangzhou, China, 25–28 October 2016; IEEE: Hangzhou, China, 2016; pp. 1518–1520. [\[CrossRef\]](#)
34. Garcia-Redondo, F.; López-Vallejo, M. Auto-Erasable RRAM Architecture Secured Against Physical and Firmware Attacks. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2018**, *65*, 1581–1590. [\[CrossRef\]](#)
35. Rakshit, J.; Mohanram, K. ASSURE: Authentication Scheme for SecURE energy efficient non-volatile memories. In Proceedings of the 2017 54th ACM/EDAC/IEEE Design Automation Conference (DAC), Austin, TX, USA, 18–22 June 2017; IEEE: Austin, TX, USA, 2017; pp. 1–6. [\[CrossRef\]](#)

36. Swami, S.; Mohanram, K. ACME: Advanced Counter Mode Encryption for Secure Non-Volatile Memories. In Proceedings of the 2018 55th ACM/ESDA/IEEE Design Automation Conference (DAC), San Francisco, CA, USA, 24–28 June 2018; IEEE: San Francisco, CA, USA, 2018; pp. 1–6. [[CrossRef](#)]
37. Rose, G.S.; Rajendran, J.; McDonald, N.; Karri, R.; Potkonjak, M.; Wysocki, B. Hardware security strategies exploiting nanoelectronic circuits. In Proceedings of the 2013 18th Asia and South Pacific Design Automation Conference (ASP-DAC), Yokohama, Japan, 22–25 January 2013; IEEE: Yokohama, Japan, 2013; pp. 368–372. [[CrossRef](#)]
38. Arumí, D.; Gonzalez, M.B.; Campabadal, F. RRAM serial configuration for the generation of random bits. *Microelectron. Eng.* **2017**, *178*, 76–79. [[CrossRef](#)]
39. Chua, L. Memristor—the missing circuit element. *IEEE Trans. Circuit Theory* **1971**, *18*, 507–519. [[CrossRef](#)]
40. Strukov, D.B.; Snider, G.S.; Stewart, D.R.; Williams, R.S. The missing memristor found. *Nature* **2008**, *453*, 80. [[CrossRef](#)]
41. Chen, Y.S.; Lee, H.Y.; Chen, P.S.; Gu, P.Y.; Chen, C.W.; Lin, W.P.; Liu, W.H.; Hsu, Y.Y.; Sheu, S.S.; Chiang, P.C.; et al. Highly scalable hafnium oxide memory with improvements of resistive distribution and read disturb immunity. In Proceedings of the 2009 IEEE International Electron Devices Meeting (IEDM), Baltimore, MD, USA, 7–9 December 2009; IEEE: Baltimore, MD, USA, 2009; pp. 1–4.
42. Yu, S.; Chen, P.-Y. Emerging memory technologies: Recent trends and prospects. *IEEE Solid-State Circuits Mag.* **2016**, *8*, 43–46. [[CrossRef](#)]
43. Lohrke, H.; Tajik, S.; Krachenfels, T.; Boit, C.; Seifert, J.-P. Key extraction using thermal laser stimulation. *IACR Trans. Cryptogr. Hardw. Embed. Syst.* **2018**, *2018*, 573–595. [[CrossRef](#)]
44. Strukov, D.B.; Stewart, D.R.; Borghetti, J.; Li, X.; Pickett, M.; Ribeiro, G.M.; Robinett, W.; Snider, G.; Strachan, J.P.; Wu, W.; et al. Hybrid CMOS/memristor circuits. In Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS), Paris, France, 30 May–2 June 2010; pp. 1967–1970.
45. Wang, H.; Shi, Q.; Nahiyani, A.; Forte, D.; Tehranipoor, M.M. A physical design flow against front-side probing attacks by internal shielding. *IEEE Trans. Comput. Aided Des. Integr. Circuits Syst.* **2019**, *39*, 2152–2165. [[CrossRef](#)]
46. Kumaran, S.; Murugan, V. Electronic Memory Using Memristors and Crossbars with Three or More in-Series Activated Memristors. U.S. Patent 9773843B2, 26 September 2017.
47. Xi, X.; Aysu, A.; Orshansky, M. Fresh re-keying with strong PUFs: A new approach to side-channel security. In Proceedings of the 2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), Washington, DC, USA, 30 April–4 May 2018; IEEE: Washington, DC, USA, 2018; pp. 118–125. [[CrossRef](#)]
48. Medwed, M.; Standaert, F.X.; Großschädl, J.; Regazzoni, F. Fresh Re-keying: Security against Side-Channel and Fault Attacks for Low-Cost Devices. In *Progress in Cryptology—AFRICACRYPT 2010*; Bernstein, D.J., Lange, T., Eds.; Springer: Berlin/Heidelberg, Germany, 2010; Volume 6055, pp. 279–296. [[CrossRef](#)]