Thermal Laser Attack and High Temperature Heating on HfO2-based OxRAM Cells

A Krakovinsky, Marc Bocquet, R Wacquez, J. Coignus, Jean-Michel Portal

Thermal Laser Attack and High Temperature Heating on HfO_2-based OxRAM Cells

A. Krakovinsky*†‡, M. Bocquet†, R. Wacquez‡, J. Coignus‡, and J-M. Portal†

***Abstract*—The last 10 years have seen the rise of new NVM technologies as alternative solutions to Flash technology, which is facing downsizing issues. Apart from offering higher performance than the state of the art of Flash, one of their key features is lower power consumption, which makes them even more suitable for the IoT era. But one of the other main concerns regarding IoT is data security, which is yet to be evaluated for emerging NVM. Our previous work aimed at putting under test the integrity of HfO_2 based resistive RAM (OxRAM cells). Bit-set occurrences were found after thermal laser attacks. This present work investigates the difference in behaviour when a selector is added to the resistive element, thanks to attack on different stacks. The results obtained give interesting tracks for the design of secure OxRAM-based ICs. It also studies the kinetic role of temperature through heating experiments.**

***Index Terms*—OxRAM, Laser, Security, Integrity, HfO_2, 1T1R, Retention, Thermal Attacks, Countermeasure.**

I. Introduction

A. Non-Volatile Memories Issues

Technologies such as Magnetic RAM (MRAM), Resistive RAM or Phase Change RAM (PCRAM) have emerged on the NVM market as possible replacements for Flash technology. Also, considering the demand for low power consumption in the upcoming IoT era, they represent serious solutions for embedded memories in smart objects. Indeed, they fit such requirements in term of cost and especially power consumption. Nonetheless, given that billions of devices containing private data will be interacting between each other in the years to come, security is also an aspect that must not be neglected.

While Flash technology is considered secured, emerging NVM integrity has not been investigated neither under UV nor laser attacks such as in [1] or [2]. This is the reason why this work is leaning on one of this technologies security issues, which is oxide-based RRAM (OxRAM).

B. OxRAM Technology Description

A 1R OxRAM cell is made of two metal electrodes with a transition metal oxide (TMO) in-between. For a better control of the current flowing through the cell, a transistor can also be added to form a 1T1R structure (as pictured on Fig. 1). Due to its small size,1R architecture is, like standalone Flash, better suited for mass storage applications. As for 1T1R structure, considering its higher reliability and performances compared to 1R cells, they can be seen as an alternative option to embedded Flash.

Data storage in OxRAM cells relies on resistance switching through redox reactions. When a voltage is applied to the top electrode in order to set a cell in a high resistive state (HRS), oxygen ions migrate from the oxide to the electrode [3]. When the set voltage V_{set} is reached, a conductive filament (CF) of oxygen vacancies is created. It enables current to flow throughout the oxide (as noticed on Fig. 2). During this operation, the current must be limited to a compliance current I_c, in order to avoid an overshoot on the cell that might drive the oxide towards a non-reversible very low resistance state. This current can be adjusted with either the measurement instrument for 1R cells or gate voltage value of the transistor for 1T1R cells.

On the contrary, if the cell is in a low resistive state (LRS), applying a voltage will make oxygen ions move back to the oxide, which is called reset. At the reset voltage (V_{Reset}) and reset current (I_{Reset}), ions begin to fill the vacancies, cut the current path, and the cell retrieve its HRS state.

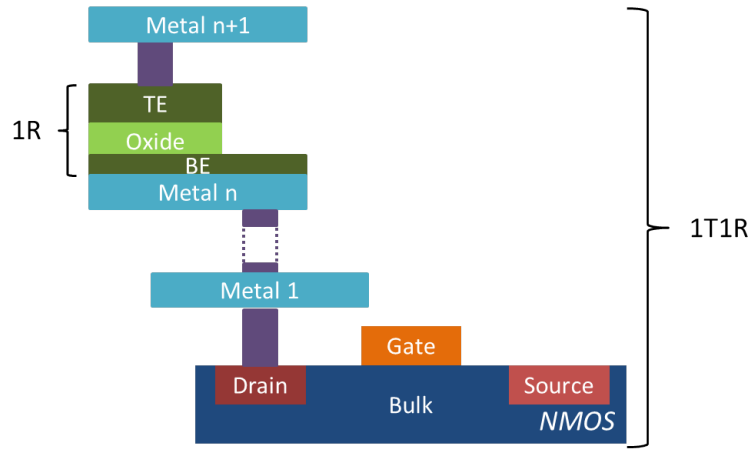

Fig. 1. Description of a 1R OxRAM stack inside a 1T1R cell architecture. In our case, the TE/Oxide/BE stack is made of Ti/HfO_2/TiN. (TE = Top Electrode, BE = Bottom Electrode)

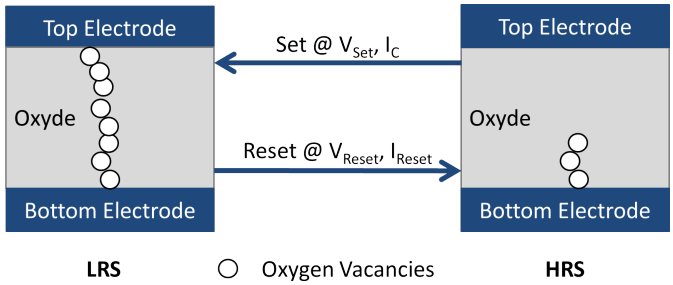

Fig. 2. Oxide structure for each state associated with resistance switching operations

*Corresponding Author - Phone Number : +33442616724 - E-mail address : alexis.krakovinsky@cea.fr

‡CEA - DRT/DPACA, Laboratoire SAS, Centre de Microélectronique de Provence, Site Georges Charpak, 880 Avenue de Mimet, 13120 Gardanne, France And CEA LETI, Minatec Campus, 17 Avenue des Martyrs, 38054 Grenoble Cedex, France

†IM2NP - UMR CNRS 7334, Aix-Marseille Université, Avenue Escadrille Normandie Niemen, Case 142, 13397 Marseille Cedex 20, France

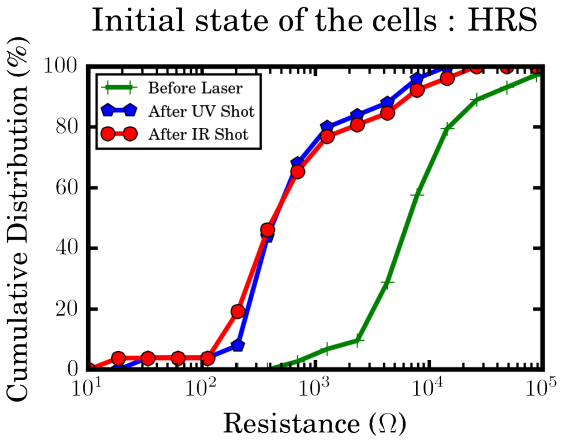

Fig. 3. Cumulative distributions of the resistance values of the 84 HRS cells before and after a single laser pulse, sorted by wavelength used (from [4])

C. Previous Results on OxRAM Cells

In our previous work presented in [4], 1R OxRAM cells made of a 5nm-thick HfO_2 layer and 10nm-thick Ti and TiN electrodes (as described in [5]) have been attacked with a Nd:YAG laser pulse. A bit-set effect has been observed on HRS-state cells (see Fig. 3), and was not influenced by the wavelengths used for the attack (*i.e* 355 nm and 1064 nm). Also, their cycling behaviour remain unchanged after the laser shot, pointing out that only data has been modified. Simulations allowed to correlate the laser influence with local temperature which reaches about 610 K at peak during the attack.

This results can also be expected on 1T1R cells, since the structure difference only impacts the compliance current management. However they are yet to be observed. Moreover, even though the temperature has been suspected for laser switching, a kinetic aspect of the heating process is not excluded. This can be verified with, for example, a much slower heating of the cells.

The following section of this paper will then be dedicated to laser attacks on 1T1R OxRAM cells. Section 3 will be focused on the effect of an oven heating of the 1R cells mentionned above, to avoid any influence from the transistor on the results.

II. Laser Attack On 1T1R OxRAM Cells

This section is focused on the switching effect occurring for HRS cells when attacked. Hence, the goal of the following experiment is to check if a change in the cell architecture impacts the qualitative aspect of the laser switching process.

A. Experimental Setup

The laser equipment used for this experiment embeds a Nd:YAG source whose wavelength is 1064 nm. The pulse has a 5μm-spot size , and a surface power up to 0,09 W.m^{-2}, with a duration that can be defined starting at 50 ns (value chosen for the following attacks). Regarding the OxRAM cells, the resistive element of the 1T1R cells is different compared to the one used in our previous work, since the oxide thickness has changed from 5 nm to 10 nm. The gate width and length of the transistors integrated in those cells are respectively W = 5 μm and L_g = 0.35 μm. As the change in oxide thickness may affect the amount of energy necessary to entirely heat the CF, the surface power value of the attack has been increased from 0,05 W.m^{-2} to 0,09 W.m^{-2}. Moreover, the experiment is conducted with a cell layout (presented in Fig. 4) that prevents the transistor from being affected by the pulse, given the size of the spot and the distance to the 1R stack.

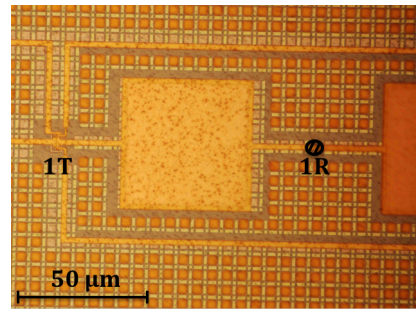

Fig. 4. Photograph of the 1T1R cell layout. The laser spot is represented by a black striped circle

TABLE I
1T1R Cells Characterisation Parameters Table

Operation	Gate	Source	Bulk	Top Electrode	Duration
Reset	2.5 V	2 V	0 V	0 V	1 µs
Set	1.1 V	0 V	0 V	2 V	1 µs
Read	3 V	0 V	0 V	0.1 V	1 µs

The electrical characterisations of the 14 HRS cells before attack consist in a quasistatic Forming operation, then two pulsed Reset/Set cycles and a pulsed Reset operation. Each operation is followed by a pulsed read of the cell state. Once the cells have been exposed to the laser, another read operation is performed as well as new pulsed Reset/Set cycles. The voltage values for each pulsed operation are given in Table I.

B. Results

B.1 Cells Resistances Values After Attack

As observed on Fig. 5, all the 14 cells under attack (HRS state) exhibit lower resistance values after the laser shot, which is consistent with previous results. There are especially 5 of these cells whose resistance is lower than the average resistance value after an electrical set, which means they switched to the LRS. However, the laser set is only reversible for one of them, since 4 cells are non-functionall (*i.e* they cannot be reset electrically after the laser pulse). They correspond to the lowest resistance values after attack of the sample. The reason why this change in architecture modifies the behaviour of these cells after attack must be investigated. We will focus on these cells that failed to reset in section B.2 .

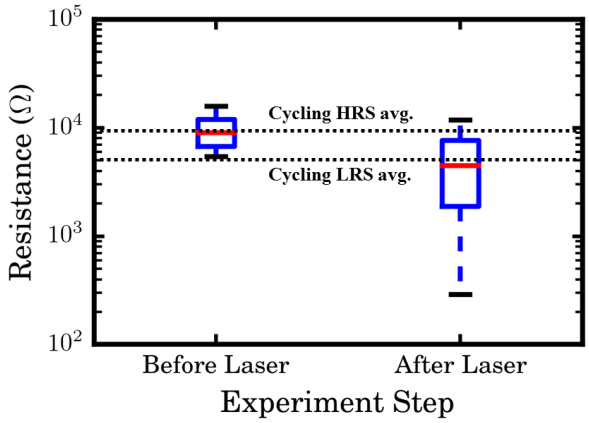

Fig. 5. Laser Impact on 1T1R HRS Cells Resistance Values. The box extends from the lower to upper quartile values of the data, with a line at the median

TABLE II
RESISTANCE VALUES OF THE CELLS THAT WERE RESET AT V_G OUT OF THE STANDARD RANGE

Resistance after laser pulse	Resistance after reset	Gate Voltage
1,7 kΩ	100 kΩ	3,2 V
3,7 kΩ	21 kΩ	3,2 V
650 Ω	200 kΩ	3,5 V
580 Ω	6 kΩ	3,5 V

B.2 Reset Failure Understanding

Despite having reset fails on these 4 cells, their resistance values (shown in Table II) are close to the ones observed for attacks on 1R cells (880 Ω average [4]). But contrary to 1T1R cells, 1R cells could be reset after the attack. One possible reason for this difference is that the reset current is not important enough to fill the vacancies of the oxide for 1T1R cells. This may be consistentl since this one is similar to the compliance current [6], and provided that I_c = 100 μA for 1T1R cells while I_c = 1 mA for 1R cells.

In order to confirm or not this hypothesis, new electrical reset operations have been performed on the four 1T1R cells that failed to reset after the attack. But this time, the gate voltage V_g (which controls I_c and thus I_{Reset}) has been increased starting at the standard value (2.5 V). This may be able to reset the cells but to overload the transistor as well.

As seen on Table II the two cells with the highest resistance values were succesfully reset at V_g = 3.2 V. The other ones switched to the HRS at V_g = 3.5 V . Aside from making the 4 concerned cells fonctionnal, this confirms our first hypothesis. This also nuances the observations made on 1R cells regarding the cell behaviour after a laser shot.

C. Implications on OxRAM design for security applications

The results of the previous section are very interesting from a security point of view. Indeed, by lowering the compliance current of the cell, the LRS resistance value is increased [7] and the reset current reduced, which means a very low resistive state might not be reversed, thus making the attack detectable.This is pictured on Fig. 6, which highlights the dependency between R_{LRS} and I_c, since a gain of a decade in resistance corresponds to a loss of about a decade in compliance current. As a consequence, working with a low compliance current, apart from being a solution to improve the consumption of low power devices, is also to take into consideration for the design of secure OxRAM-based ICs.

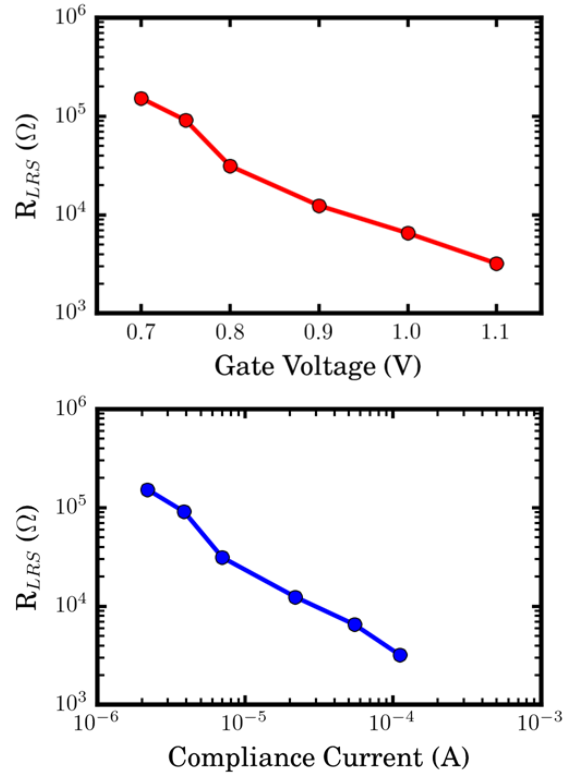

Fig. 6. LRS level for different values of I_c and V_g

There are two ways to lessen the compliance current value in OxRAM cells. The first is the most obvious one, which is to reduce the gate voltage value V_g, since it lowers the drain current as well, and therefore the cell current (since the cell is connected to the drain as pictured in Fig. 1), as noticed on Fig. 6.

The other method consists in reducing the transistor gate size, which has a direct influence on the compliance current. In our case, regular cycling performed on devices with different values of W pointed out that dividing the gate width by 20 allows to lower the compliance from about a decade. This method appears to be safer since one cannot modify the size of the transistor while the gate voltage can be changed.

D. Conclusion

As expected, a bit set effect has been obtained on about 40% of the targeted 1T1R cells. Nonetheless, the resistance of a cell after attack is lower than the resistance obtained after an elec-

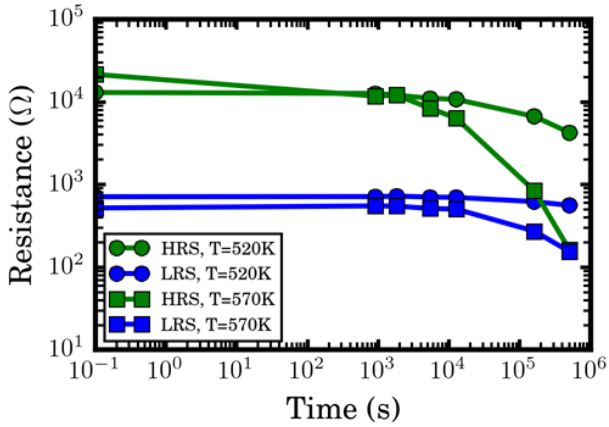

Fig. 7. Average resistance values evolution through time of 16 1R OxRAM cells at 520 K and 570 K

trical set. In other words, the CF created is bigger during a laser attack than it is while the cell is cycled. As a consequence, a higher value of I_{reset} (and thus I_c) is required to reset the cell. Therefore, the use of a low compliance current, provided by a smaller gate of the transistor, seems to be an interesting track for a countermeasure against this kind of attack, since it would allow to detect the creation of a large conductive filament within the oxide of the cell.

III. High Temperature Oven Heating

Our previous work has shown that a laser pulse could impact the cells independently from the wavelength used. We also demonstrated that as the metallization layer above the resistive element absorbs all the induced photons (transmission coefficient $\approx 10^{-15}$ for λ = 1064 nm and about 10^{-24} for λ = 355 nm), temperature only is responsible for the bit-set effect on HRS cells. Which is consistent with the results of the laser heating and electrical set models that were implemented [4].

While a laser attack provides a brutal heating to the device, a slow increase of the temperature might not have the same effect. The goal here is thus to observe what could happen if a gradual rise of the temperature (*i.e* with an oven heating) was performed on the cells.

A. Experimental Setup

In order to avoid any influence from the transistor on the results, this experiment has been conducted on 1R cells. These OxRAM devices are the same 1R cells that were studied in [4]. 16 HRS and 16 LRS cells have been characterised before (few set/reset cycles) and after being heated at a temperature T. The chosen temperatures for the experiment are T_{Heat1} = 520 K and T_{Heat2} = 570 K. Several read operations have been performed on the cells to monitor their resistance value. The total time the devices spent in the oven is about a week.

B. Heating Results

As represented on Fig. 7, an important variation of the resistance values can be highlighted on all HRS cells at both temperatures. At T_{Heat1}, both HRS and LRS are stable until three hours. The average HRS resistance value is highly impacted afterwards since it changes from 13 kΩ to 4 kΩ, though the cells are not switching to the LRS. The LRS average resistance level is also slightly decreasing. This is something that had been unnoticed for laser attacks.

This tendency is even more visible by looking at the curves for T=T_{Heat2}. After being stable for about 20 minutes, all the HRS cells have switched to the LRS. In addition, the decay in LRS resistance average value is getting more important as it varies from 500 Ω to 180 Ω. Another important result is that both HRS and LRS states are merging towards the same resistance level R_{Heat2} = 180 Ω . However, given the low value obtained, none of these cells could be reset (with standard parameters) afterwards with I_c = 1 mA.

The effects obtained on the cells are consistent with the simulated laser temperature mentionned in Section 1, but they discard the hypothesis of a kinetic-driven process. However, the LRS of all cells has also been impacted, while it was not the case during laser experiments. This implies that a higher laser surface power might have influenced the devices in a similar way.

C. Improving Thermal Laser Attacks

This results also give a track for a possible imporvement of the attack performed in Section II. Indeed, one can remark that the cells are being set progressively. Hence, lessening the oven time would have left the cells in a higher state. The same observation can be made for the temperature, since for an equal baking duration, the higher the temperature, the lower the resistance value. This reasoning could also be applied to a laser pulse.

As a result, in the best case scenario for an attacker, this means that an accurate control of the duration and the surface power of the laser pulse (which is correlated with the heating temperature) could leave a cell in any desired state below the HRS. If the control of the resistance value after attack can be achieved, the countermeasure presented at the end of Section II would be invalidated.

IV. Conclusion

It has already been shown that a laser attack could set an OxRAM cell. However, while 1R cells were still functional afterwards, some 1T1R cells could not be reset since the reset current was not sufficient to switch the cells back to the HRS. This has been explained by the use of a lower compliance current for 1T1R cells compared to 1R cells. Hence, working at a low compliance current can be seen as a countermeasure to laser attacks, and can be achieved by either lowering the gate voltage or reducing the size of the gate.

A heating experiment also allowed to confirm the results of thermal and electrical simulations, that were performed in a previous work, regarding the laser set temperature. It also rejects the possibility of a set induced by a brutal heating exclusively. In other words temperature only is able to make the ions migrate from the oxide to the top electrode of an OxRAM stack. This progessive switch of the oxide state can be exploited to improve the laser attack which could lead to a control of the resistance

value after attack, which can bypass the previously found countermeasure.

REFERENCES

[1] Schmidt et al., *Optical Fault Attacks on AES: A Threat in Violet* Hardware-Oriented Security and Trust, 2009. HOST '09. IEEE International Workshop on , vol., no., pp.1-6, 27-27 July 2009

[2] Skorobogatov, S., *Local Heating Attacks on Flash Memory Devices* 2009 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC), Lausanne, 2009, pp. 13-22

[3] Nardi et al. , *Resistive Switching by Voltage-Driven Ion Migration in Bipolar RRAMPart I: Experimental Study,* in Electron Devices, IEEE Transactions on , vol.59, no.9, pp.2461-2467, Sept. 2012

[4] Krakovinsky et al. , *Impact of a laser pulse on HfO2-based RRAM cells reliability and integrity,* 2016 International Conference on Microelectronic Test Structures (ICMTS), Yokohama, 2016, pp. 152-156

[5] Vianello et al. , *Resistive Memories for Ultra-Low-Power embedded computing design,* in Electron Devices Meeting (IEDM), 2014 IEEE International , vol., no., pp.6.3.1-6.3.4, 15-17 Dec. 2014

[6] D. Ielmini et al., *Universal Reset Characteristics of Unipolar and Bipolar Metal-Oxide RRAM* in Electron Devices, IEEE Transactions on , vol.58, no.10, pp p.3246-3253, Oct. 2011

[7] Nardi et al., *Control of filament size and reduction of reset current below 10A in NiO resistance switching memories* in Solid-State Electronics, 58(1) : 4247, apr 2011. doi:10.1016/j.sse.2010.11.031.

Acknowledgements :

This work was performed with the support of the CATRENE CA208 Mobitrust project.