Microprocessors and Microsystems 87 (2021) 104376

Contents lists available at ScienceDirect

Microprocessors and Microsystems

journal homepage: www.elsevier.com/locate/micpro

Sensitivity of HfO_2-based RRAM Cells to Laser Irradiation

Dmytro Petryk [a,*], Zoya Dyka [a], Eduardo Perez [a], Ievgen Kabin [a], Jens Katzer [a], Jan Schäffner [a], Peter Langendörfer [a,b]

[a] IHP – Leibniz-Institut für innovative Mikroelektronik, Frankfurt (Oder), Germany
[b] BTU Cottbus-Senftenberg, Cottbus, Germany

ARTICLE INFO

Keywords:
Optical Fault Injection attack
Laser
Reliability
Security
RRAM
Memristive devices
Resistive switching
1T-1R

ABSTRACT

Today, the technology of resistive random access memory is used as a non-volatile memory. In this paper we investigate in details the sensitivity of the TiN/Ti/Al:HfO_2/TiN-based 1T-1R resistive random access memory cells implemented in a 250 nm CMOS IHP technology to the laser irradiation. Experimental results show that the laser irradiation can influence the resistive state of RRAM cells significantly, i.e. precisely localized optical faults can be successfully injected. We focus on the selection of the configurable parameters of the laser station and their influence on the success of optical Fault Injections. Additionally, we localize sensitive areas of attacked chips. Based on the determined sensitive areas we show that metal fillers atop memory cells influence on success of optical fault injection attacks.

1. Introduction

The use of single-level memory was discussed in computer science/computer engineering already in the early 1970. The core idea is that there is a non-volatile resistive random access memory (RRAM) that allows fast read and write access using low power only. In 1971 such a memristive semiconductor device was postulated [1]. In addition, more than 50 years ago it has been shown that under electrical stress metal oxides exhibit a transition from an electrically insulating to a conducting state, and vice versa [2, 3]. This phenomenon, referred to as resistive switching [3], triggered the goal to develop a universal memory [4], which experienced a revival in the 1990s reviving the idea of computer systems with single-level memory based on non-volatile random access memory and fostering again research in that area [5, 6]. Due to its reduced power consumption compared to flash, RRAM is especially attractive for realizing industrial control systems, smart cities, battery powered devices for e-health, the Internet of Things (IoT) and the like. In all these areas security is paramount but devices normally do not have sufficient protection means to resist physical attacks. These smart devices are physically accessible. Hence, they can be stolen and analyzed/manipulated in a laboratory specialized on side-channel analysis and/or fault injection (FI) attacks. So, the behavior of RRAM cells under attack is very important from a security point of view. Our interest to RRAM is due to its inconsistent reaction to laser irradiation. Particularly, it is not known if a specific RRAM implementation is or is not sensitive to physical attacks, e.g. optical FIs. If not, it might be suitable for realizing IoT devices. Conversely, if it is sensitive to laser-based attacks, it is important to know the reason why and which areas of the chip are sensitive in order to propose countermeasure(s).

Some papers discussing the sensitivity of RRAM cells to laser irradiation have already been published. A detailed description of these results and comparison with results obtained in this work are given in section VIII.

In this paper we investigate the sensitivity of IHP RRAM cells to laser irradiation. This paper extends the research published in [36] by determining the sensitive areas of IHP RRAM chips and the influence of metal fillers on the success of optical FI attacks. The main contributions of this paper are:

- we show the feasibility to influence the state of individual cells in an IHP RRAM chip;
- we discuss the possible reasons for the success of the performed attack and demonstrate that it depends at least partially on the placement of metal fillers on top of the RRAM cell;
- we discuss the use of metal fillers as low-cost countermeasure against optical FI attacks. On the one hand, metal fillers seem to be an

* Corresponding author.
E-mail addresses: petryk@ihp-microelectronics.com (D. Petryk), dyka@ihp-microelectronics.com (Z. Dyka), perez@ihp-microelectronics.com (E. Perez), kabin@ihp-microelectronics.com (I. Kabin), katzer@ihp-microelectronics.com (J. Katzer), schaeffner@ihp-microelectronics.com (J. Schäffner), langendoerfer@ihp-microelectronics.com (P. Langendörfer).

https://doi.org/10.1016/j.micpro.2021.104376
Received 22 December 2020; Received in revised form 26 August 2021; Accepted 24 September 2021
Available online 2 November 2021

effective countermeasure as they are blocking the laser beam. Knowledge about the sensitive areas of a single RRAM cell to laser irradiation can be used for placement of metal fillers, as part of design rules in the layout tool. On the other hand, our experiments show that the Metal-Insulator-Metal (MIM) structures covered by metal fillers as well as the MIM structures that are not covered by metal fillers were successfully influenced. That makes the use of metal fillers as a low-cost countermeasure rather questionable.

The paper is structured as follows. Section II describes the phenomena of resistive switching, the structure of the attacked IHP RRAM chip and the measurement equipment to operate an IHP RRAM chip. Section III discusses the analysis of the influence of the READ operation on the RRAM cell state and presents our criterion of successfully influencing them by a laser. Section IV describes the equipment used to perform optical Fault Injection attacks. Section V presents the preliminary preparations of the attacked chips before the optical Fault Injection experiments. Section VI shows the results of optical Fault Injection attacks on IHP RRAM chips. Section VII describes our analysis of sensitive areas of IHP RRAM chips. Section VIII presents the comparison of the obtained results with other published works. Section IX concludes this work.

2. Background basics: RRAM

2.1. Resistive switching and RRAM cell architecture

RRAM is an emergent non-volatile memory technology, also known as a particular implementation of memristors, that is based on the phenomena of resistive switching. Resistive switching is the physical phenomenon that uses a non-volatile and reversible change of the resistance due to the application of electric stress, typically voltage or current pulses [3, 4, 14]. Typical resistive switching systems are capacitor like devices, where the electrodes are a metal and the dielectric is a transition metal oxide with insulator properties. Transition metal oxide is a compound consisting of oxygen atoms bound to transition metal ones[1]. Transition metal oxides are interesting because of their wide range of electrical and magnetic properties [15]. Resistive switching in a transition metal oxide with insulator property allows to use a MIM structure as a memory element.

Resistance change in a MIM structure is achieved by formation or rupture of nanosized conducting filamentary path (further denoted as "conductive filament") in a transition metal oxide. Fig. 1 shows schematically the MIM structure with formed and with ruptured conductive filament.

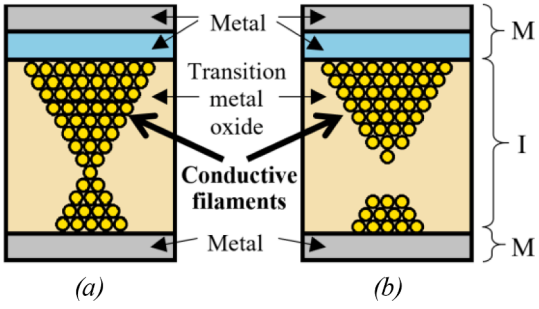


Fig. 1. Metal-Insulator-Metal structure with conductive filament in transition metal oxide: *(a)* – formed conductive filament establishes the connection between top and bottom metal, i.e. the MIM structure is in a low resistive state; *(b)* – ruptured conductive filament, the connection between top and bottom metal is not established, i.e. the MIM structure is in a high resistive state.

The conductive filament in a transition metal oxide establishes the connection between top and bottom metal electrodes for the current flow, see Fig. 1–*(a)*. It is the state with a high conductivity level, i.e. it is a Low Resistive State (LRS). This state is associated with an ON state. Please note that formed conductive filament may have different thicknesses that subsequently influence the conductivity of MIM structure. Due to this fact LRS can be divided into several states [38] if stable switching between these levels is ensured. The version of IHP RRAM we used for our experiments currently supports only two stable states, i.e. LRS and HRS. Hence, we consider two logical states only, i.e. HRS and LRS in *II-A* and *II-B*.

Rupture of the conductive filament (see Fig. 1–*(b)*) disconnects the top electrode from the bottom electrode that significantly reduces the current flow through the transition metal oxide. It is the state with a low conductivity level, i.e it is a High Resistive State (HRS). This state is associated with an OFF state.

Due to the fact that a MIM structure has at least two stable states – the LRS and the HRS – it can be used as a memory element for the storing 1 bit of information. LRS is usually considered as a logical state '1'. HRS is usually considered as a logical state '0'. Thus, theoretically an RRAM cell can be developed based on a MIM structure if the switching from one logical state to another and vice versa is possible, manageable, controllable and reliable. This switching can be unipolar or bipolar:

- Unipolar: the switching between two stable states does not depend on the polarity of the operating voltage [4].
- Bipolar: the switching between stable states depends on the polarity of the operating voltage [4], i.e. switching from HRS to LRS (further denoted as HRS → LRS) has one polarity and switching from LRS to HRS (further denoted as LRS → HRS) has the opposite polarity.

Similar behavior of many RRAM cells and low manufacturing costs are additional requirements for the mass production of memory chips based on RRAM cells. Recently, the resistive switching phenomenon was observed in a wide variety of materials suitable for RRAM [18] such as chalcogenides[2] and perovskite-type oxides[3], binary transition metal oxides[4]. These materials are compatible with fabrication processes that are economically efficient. These materials are used for manufacturing commercial RRAM chips, for example by Panasonic [19], Fujitsu [20], Adesto Technologies [21], etc.

In this work we investigate IHP RRAMs [22] manufactured in the IHP CMOS 250 nm technology [23, 37]. Details about the switching behavior can be found in [13, 18].

The IHP RRAM cell is based on a 1 Transistor 1 Resistor (1T-1R) architecture, i.e. an RRAM cell consists of a transistor and a MIM structure in series. The MIM structure is built on a TiN/Ti/Al doped HfO_2 (Al:HfO_2)/TiN stack and manifests a bipolar resistive switching. The Ti layer is used to increase the performance and reliability in RRAM cells [24], i.e. operating voltages, retention, endurance, etc. In addition the MIM structure should have some asymmetry to exhibit bipolar resistive switching. The Ti layer provides this asymmetry. This is corroborated with the results presented in [25] where the authors reported that absence of the Ti layer in TiN/HfO_2/TiN stacks leads to unreliable bipolar resistive switching.

Fig. 2 shows a cross-sectional transmission electron microscopy image of an IHP RRAM cell (see Fig. 2–*(a)*) with the MIM structure, zoomed in (see Fig. 2–*(b)*).

The MIM structure is located on Metal 2 layer and connected to the

[1] Transition metal is a metal with incomplete d sub-shell [16], i.e. it is any metal in groups from 3 to 12 of the periodic table. More details about the d sub-shell, electronic configuration and atom orbitals can be found in [17].

[2] chemical compounds, e.g. SiS_2, B_2S_3, Sb_2S_3.

[3] chemical compounds, e.g. $CaTiO_3$, $MgSiO_3$, Fe SiO_3.

[4] chemical compounds, e.g. TaO_5, TiO_2, and HfO_2.

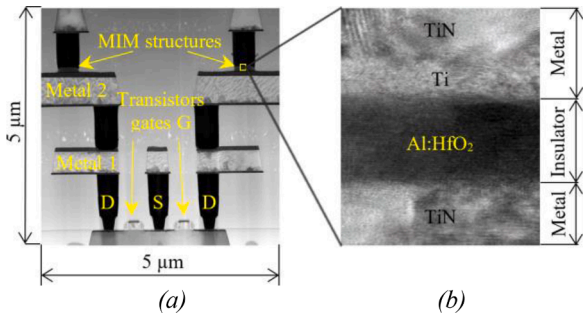


Fig. 2. A cross-sectional transmission electron microscopy image of an IHP RRAM cell: *(a)* – the MIM structure with a transistor; *(b)* – the MIM structure, zoomed in.

drain of the access transistor through vias[5].

An equivalent electrical circuit of an RRAM cell based on 1T-1R architecture is shown in Fig. 3. The variable resistor in Fig. 3 represents the MIM structure in an RRAM cell. The RRAM cell is operated by applying voltages to three electrodes. These voltages are:

- V_{BL} – *Bit Line (BL)* voltage;
- V_{WL} – *Word Line (WL)* voltage;
- V_{SL} – *Source Line (SL)* voltage.

The transistor in the IHP RRAM cell is an N-channel Metal-Oxide-Semiconductor (NMOS) Field-Effect Transistor (FET) (see Fig. 3) that has two functions:

- Limitation of current through the MIM structure;
- Accessibility to a cell.

Limiting the current through the MIM structure is necessary to prevent the MIM structure from a hard breakdown. A hard breakdown occurs due to a significant change in current or voltage during electric stress. Due to this stress conductive filaments are formed in the transition metal oxide. It is very hard to rupture these filaments afterwards. There is also a soft breakdown that results in much smaller changes of current or voltage during electric stress. Subsequently, formed conductive filaments can be easier ruptured and recovered in the transition metal oxide.

2.2. Physical processes at the Ti/Al:HfO_2 interface

There is a large diversity of physical phenomena that may lead to resistive switching. In this work we describe only one class that exploits electrochemical effects, particularly the valence change mechanism. Details about other classes can be found in [4]. The valence change mechanism relates to the oxidation-reduction (redox) processes in the MIM structure, particularly in transition metal oxides. The resistance of a transition metal oxide depends on certain oxygen stoichiometry[6]. Redox processes in the case of the valence change mechanism are provoked by an electrical voltage. This valence change is associated with a migration of oxygen vacancies in transition metal oxides, e.g. in an Al:HfO_2 layer. This change of the stoichiometry leads to a redox reaction that subsequently affects the conductivity of the material. Oxidation or reduction processes can be determined by the applied voltage polarity in case of bipolar resistive switching. Commonly the switching mechanism is described by the defects in a material, particularly the Frenkel defect [26]. This defect is a point defect in a crystal lattice when an atom leaves the lattice site and places itself in an interstitial position. This creates a vacancy in the lattice site. The ion that leaves the lattice site and the formed vacancy are called a Frenkel pair. In case of the HfO_2 layer Frenkel defects create the oxygen anions and the oxygen vacancies with charge states of 2- and 2+ respectively. Depletion or enrichment of the vacancies in a material changes the valence, i.e. affects the material conductivity. In the following we focus on describing the conductive filament forming/rupture processes that occur in the IHP MIM structure. Fig. 4 shows the migration of Frenkel pairs in the TiN/Ti/Al:HfO_2/TiN stack.

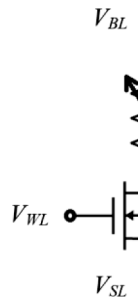


Fig. 3. Equivalent electrical circuit of 1 Transistor-1 Resistor architecture of an IHP RRAM cell.

The Ti layer acts as a scavenging layer for the oxygen atoms. After manufacturing of the IHP RRAM the Al:HfO_2 has a gradient of vacancies that are concentrated closely to the Ti layer at the Ti/Al:HfO_2 interface, i.e. Frenkel pairs are created, see Fig. 4–*(a)*. Applying a direct electric field causes the generation of additional Frenkel pairs at the Ti/Al:HfO_2 interface, see Fig. 4–*(b)*. Under a direct electric field the oxygen anions migrate in the Ti layer and accumulate there with a higher density at the Ti/Al:HfO_2 interface. The migration of oxygen anions into the Ti layer can be associated with the reduction process. Reciprocally the formed oxygen vacancies inside the Al-doped HfO_2 layer are associated with an oxidation process. Simultaneously with the migration of oxygen anions the oxygen vacancies migrate inside the Al:HfO_2 layer to the TiN bottom electrode gathering there. As a consequence the oxygen vacancies create a conductive filament. According to the fabrication process, the growth direction of the conductive filament is from the anode (TiN top electrode) to the cathode (TiN bottom electrode), see Fig. 4–*(b)*. The details about the influence of the fabrication process on the conductive fila-

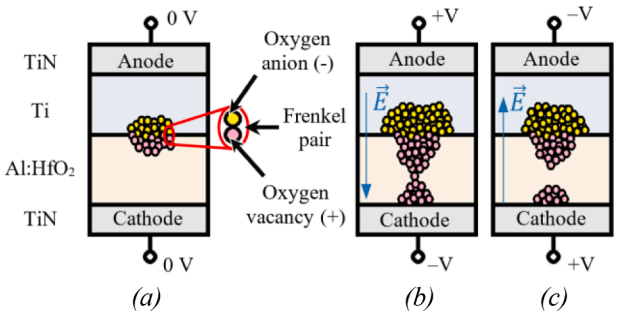


Fig. 4. Illustration of the MIM structure with dislocation of oxygen anions and vacancies: *(a)* – distribution of anions and vacancies at the Ti/Al:HfO_2 interface after manufacturing; *(b)* – formation of a conductive filament, i.e. SET operation; *(c)* – rupture of a conductive filament, i.e. RESET operation.

[5] Interconnectors between metal layers.

[6] in chemistry the stoichiometry denotes the ratio between an amount of reagents in a reaction and the amount of the products [17]. This ratio is expressed by the use of natural numbers.

ments growth direction can be found in [26]. The formation of the conductive filament in MIM structure is denoted as SET operation. When applying a reverse electric field the oxygen anions at the Ti/Al:HfO_2 interface may recombine with the oxygen vacancies, i.e. the reduction of the conductive Al-doped Hf in the Al:HfO_2 layer starts. Simultaneously the Ti layer is oxidized by the loss of the oxygen anions. As a consequence the conductive filament is ruptured, see Fig. 4–*(c)*. The rupture of the conductive filament is denoted as RESET operation. Note that a formation of conductive filament is not a completely predefined process due to the randomness of defects in the crystal lattice. Also the interaction of Ti and Al:HfO_2 layers at the Ti/Al:HfO_2 interface have non-stoichiometric behavior due to the undefined ratio of the reaction product and this ratio cannot be shown in natural numbers[7]. Due to these facts the thickness of conductive filament may vary from cell to cell. It causes significant changes in the conductivity when applying equal voltages to the cells.

2.3. Operating modes of RRAM cells

After fabrication the MIM structure is in pristine state and the insulator conducts a low level of current. The resistive switching of the RRAM cells has to be initiated by a special operation called ELECTROFORMING that is a kind of a soft breakdown. Other operations with the RRAM cells are:

- READ: the recognition of the cell state.
- RESET: changing the resistance level of the cell from the Low Resistive State to the High Resistive State (LRS → HRS).
- SET: changing the resistance level of the cell from the High Resistive State to the Low Resistive State (HRS → LRS).

Thus, the operations SET and RESET are write operations. The rest of this section describes the ELECTROFORMING, SET, RESET and READ operations in detail. These operations are performed using a special setup that we describe in section *II-E*. To perform ELECTROFOMING/SET/RESET operations the Incremental Step Pulse with Verify Algorithm (ISPVA) is used. Details about the ISPVA can be found in [27]. We start with the description of the READ operation, because this operation is the most used operation.

The READ operation is executed by applying $V_{WL} = 1.4$ V, $V_{SL} = 0$ V and $V_{BL} = 0.2$ V, see Fig. 3. All applied voltages are constant values. The output of the READ operation is a measured value of the current I that flows through the cell. The value I allows to determine the state of the cell:

- if 0 μA $\leq I \leq$ 5 μA – the cell is in HRS;
- if 5 μA $< I <$ 30 μA – the cell is in an undefined state;
- if 30 μA $\leq I \leq$ 50 μA – the cell is in LRS;
- if 50 μA $< I \leq$ 100 μA – the cell is stuck in LRS;

ELECTROFORMING is the operation applied to each RRAM cell after its manufacturing. This operation plays an important role in the subsequent performance of the RRAM cell. ELECTROFORMING is performed only once. To perform this operation the *Word Line voltage* is connected to 1.4 V ($V_{WL} = 1.4$ V), the *Source Line voltage* to 0 V ($V_{SL} = 0$ V) and the *Bit Line voltage* V_{BL} should be changed in a range from 2 V to 5 V with a step of 0.01 V increasing for each attempt. This operation usually requires more than one attempt. The first attempt starts with $V_{BL} = 2.00$ V. After each attempt the READ operation is performed to determine the current state of the cell. If the measured current through the cell reached 30 μA the conductive filament is formed, i.e. the cell is considered as ELECTROFORMed and ELECTROFORMING stops for this cell. Otherwise the next attempt has to be done with increasing value of the voltage V_{BL} till a value of $I \geq 30$ μA is reached or the V_{BL} value reaches 5 V. If resistive switching behaviour is still not achieved by $V_{BL} = 5.00$ V the cell can be defined as *broken*.

To perform the RESET operation the *Word Line voltage* is connected to 2.7 V ($V_{WL} = 2.7$ V), the *Bit Line voltage* to 0 V ($V_{BL} = 0$ V) and the *Source Line voltage* V_{SL} should be changed in a range from 0.5 V to 3.5 V with a step of 0.1 V increasing for each attempt. This operation usually requires more than one attempt. After each attempt the READ operation is performed. If the value of the current through the cell is low, i.e. $I \leq 5$ μA the cell is in the HRS and the RESET operation stops. Otherwise the next attempt has to be done. If the current through the cell after last attempt, i.e. applying the voltage $V_{SL} = 3.5$ V, is still high, i.e. $I > 5$ μA, the cell can be defined as *broken*.

To perform the SET operation the *Word Line voltage* is connected to 1.4 V ($V_{WL} = 1.4$ V), the *Source Line voltage* to 0 V ($V_{SL} = 0$ V) and the *Bit Line voltage* V_{BL} should be changed in a range from 0.5 V to 3.5 V with a step of 0.1 V increasing for each attempt. The first attempt starts with $V_{BL} = 0.5$ V. If the value of the current through the cell after an attempt is high, i.e. $I \geq 30$ μA, the cell is in the LRS and the SET operation stops. Otherwise the next attempt has to be done, till the current through the cell is $I \geq 30$ μA or the V_{BL} value reaches 3.5 V. If the current through the cell after applying the voltage $V_{BL} = 3.5$ V is still not high enough, i.e. $I <$ 30 μA the cell can be defined as *broken*.

Please note that the definition of the broken cells depend on the definitions of the HRS and the LRS of the cells. Additionally, it has to be taken into account that some broken cells are not really broken but only stressed and can get to working values over next operations. Due to these facts and our experiments we used in this work the following definition for broken cells:

- the cells with I > 1 μA before ELECTROFORMING;
- the cells with $I <$ 5 μA after ELECTROFORMING or after SET operations.

Once we identified broken cells in the attacked chip we excluded these cells from the evaluation in this work.

2.4. Attacked IHP RRAM chip

RRAM cells are organized as an array, see Fig. 5.

Each single RRAM cell in such an array is connected to *Bit Line* BL_i, *Word Line* WL_j and *Source Line* SL_k. In this work we denote cells that are connected to the WL_j and BL_i further as cells with "coordinates" (WL_j, BL_i), see Fig. 5. Applying voltage to a *Source Line* determines a kind of operation: RESET (if $V_{SL} \neq 0$ V) or one of the other operations (if $V_{SL} =$ 0 V), i.e. ELECTROFORMING, READ or SET. Thus, each single RRAM

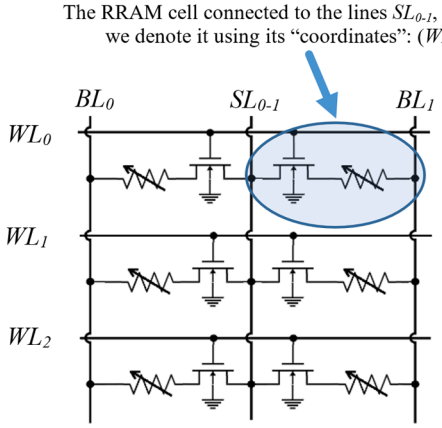


Fig. 5. Electrical circuit of six RRAM cells organized as an array.

[7] Usually in the literature this non-stoichiometry is shown as HfO_{2-X} for the HfO_2 layer.

cell can be addressed for the selected operation by applying voltages V_{BL} to the *Bit Line* BL_i, V_{WL} to the *Word Line* WL_j and V_{SL} to the *Source Line* SL_k explicitly. For example, if the *Bit Line* BL_1 is connected to $V_{BL} = 0.2$ V, the *Word Line* WL_0 to $V_{WL} = 1.4$ V and *Source Line* $SL_{0\text{-}1}$ to $V_{SL} = 0$ V, the RRAM cell (WL_0, BL_1) is selected for the READ operation. If the *Bit Line* BL_1 is connected to $V_{BL} = 0$ V, the *Word Line* WL_0 to $V_{WL} = 2.7$ V and *Source Line* $SL_{0\text{-}1}$ to $V_{SL} = 2$ V, the RRAM cell (0, 1) is selected for the RESET operation. The layout of *Bit Lines, Word Lines* and *Source Lines* will be further kept in this work as it is shown in Fig. 5, i.e. *Bit Lines* and *Source Lines* are vertical lines (further columns) and *Word Lines* are horizontal lines (further rows).

IHP manufactures chips with an RRAM array which contains the 64 *Word Lines* and the 64 *Bit Lines*, i.e. this array contains 64×64=4096 RRAM cells. This array can be used for storing 4 kbit of information. The layout of a 4 kbit IHP RRAM array is shown in Fig. 6 with a part of the layout containing only 6 RRAM cells, zoomed in.

The part of the layout with 6 RRAM cells that is shown in Fig. 6–*(a)* corresponds to the electrical circuit shown in Fig. 5. The RRAM cell marked with a circle in Fig. 5 is marked with a rectangle in Fig. 6–*(a)*.

In order to control the voltages V_{WL}, V_{BL}, V_{SL} and measure the current through the addressed cell the following blocks were designed at IHP [23]:

- *word* address decoder (XDC Mux).

It is a 6-in/64-out decoder that selects a single word line *WLj* from the 64 word lines.

- *bit* address decoder (YDC Mux).

It is a 6-in/64-out decoder that selects a single bit line *BLi* from the 64 bit lines.

- operation control circuit (Mode).

The 4 kbit memory arrays with these control blocks are denoted further as 4 kbit memory structures.

Fig. 7 shows the layout of the IHP RRAM chip with two 4 kbit memory structures. In this work all experiments were performed with only one structure that is marked in Fig. 7–*(a)* with the yellow rectangle. This structure is shown in Fig. 7–*(b)* zoomed in.

Due to the fact that only 1 memory structure was selected for the experiments we call the IHP chip further "4 kbit RRAM".

The 4 kbit RRAM chip is placed in a TQFP64 package with 64 pins. The package material is a ceramic. This package consists of 3 parts: a cap, a middle frame and a base. In order to perform laser experiments the access to the chip surface should be available. Thus the cap of the package was removed with a hot air work station for PCBs. Fig. 8 shows a 4 kbit RRAM chip in a package with a cap (see Fig. 8–*(a)*) and without

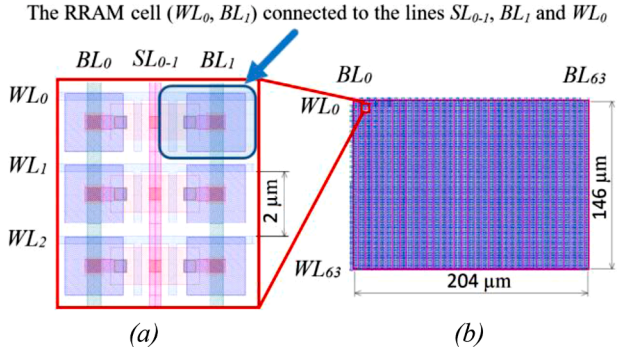


Fig. 6. Layout of an IHP 4 kbit RRAM chip: *(a)* – a part of the array with 6 RRAM cells, zoomed in; *(b)* – a 4 kbit memory array.

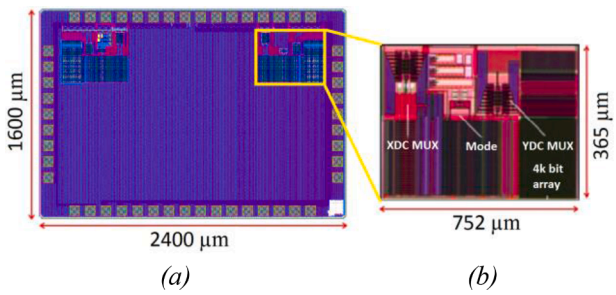


Fig. 7. Layout of the IHP RRAM chip: *(a)* – the RRAM chip with two 4 kbit memory structures, the structure selected for our experiments is marked with yellow rectangle; *(b)* – 4 kbit memory structure, zoomed in.

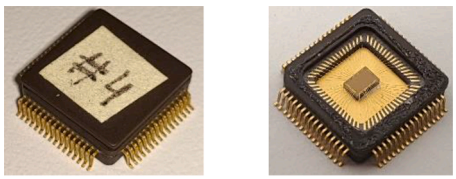


Fig. 8. A 4 kbit RRAM chip: *(a)* – the chip in the package; *(b)* – the chip in the package after removing the cap.

a cap (see Fig. 8–*(b)*).

For successfully removing the cap we heated the chip for 15 s with a temperature of 450 °C. After the cap removal we made a visual inspection to check if the bonding wires still intact and the chip surface is clean. After the chip had been tested for functionality, it was programmed.

2.5. Measurement setup and representation of the measured data

To operate a packaged 4 kbit RRAM chip a special setup is used, see Fig. 9. This device is a Non Volatile Memory Tester named RIFLE SE manufactured by Active Technologies [28]. Fig. 9 shows the RIFLE SE operating device (see Fig. 9–*(a)*) and a PCB with a socket for a 4 kbit RRAM chip (see Fig. 9–*(b)*), zoomed in.

Due to the big size of the RIFLE SE setup (90 cm × 75 cm) it is impossible to place it into the box with the laser, see Fig. 13. This limits the experiments that can be performed, e.g. the influence of the laser *during* the READ, ELECTROFORMING, RESET and SET operations cannot be measured. Therefore, we first measured the currents through the RRAM cells, i.e. we performed the READ operation for each cell, after that we performed the laser scans and then we measured the currents again and compared the values of the current before and after the laser scan. The output of the performed READ operation using the RIFLE

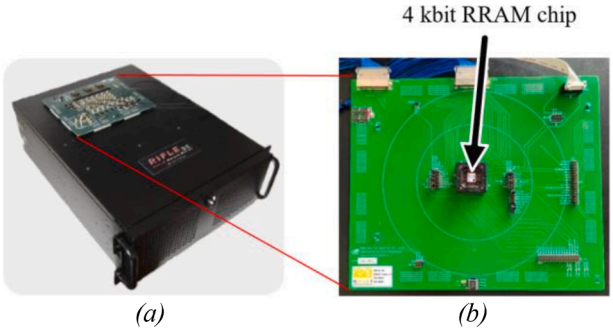


Fig. 9. Operating device for a 4 kbit RRAM chip: *(a)* – Active Technologies RIFLE SE; *(b)* – a PCB with a socket for a 4 kbit RRAM chip.

SE setup is a text file (*.txt). This file contains 64×64 values of the current *I* through each of the 4096 cells, i.e. it is a two-dimensional array corresponding to the RRAM cells topology. We denote this array further as matrix of Measured Currents (*MC*). A part of the *MC*-matrix of an RRAM chip is shown in Fig. 10.

Each value in an *MC*-matrix is a measured value of current (*I*) through an RRAM cell in the range from 0 μA up to 100 μA. We represented each value in an *MC*-matrix using a color scale from blue to yellow. A blue color represents cells with low current (i.e. about 0 μA), i.e. it corresponds to the cells in the HRS. A yellow color represents the cells with high current (i.e. about 100 μA), i.e. it corresponds to the cells in the LRS. In this work we denote the colorized *MC*-matrix as matrix of Visualized Currents (*VC*), see for example a part of the *VC*-matrix in Fig. 10.

The 4 kbit RRAM chips have a high inter-cell variability [29]. This variability is due to the manufacturing process that does not allow to produce cells with ideal similarity and stochastic nature of the switching operations. Thus the color of the cells in the *VC*-matrix after ELECTROFORMING are not only blue and yellow but green as well, see Fig. 10.

Since the values of the measured current *I* determine the state of the cell (see section *II-C*) we associate them to digital states as follows:

- '0' – the cell is in HRS;
- 'undefined' – the cell is in an undefined state;
- '1' – the cell is in LRS;
- 'Stuck-at 1' – the cell is stuck in LRS;

Hence, we can represent a matrix of measured currents as a *State matrix*. The *State matrix* represents the broken (white) cells and the cells of the other four possible states: logical '0' (orange), logical '1' (violet), undefined (red), 'Stuck-at 1' (light blue), see Fig. 10.

Fig. 11 shows the *VC*-matrices of the 4 kbit memory array of the chip #6 before ELECTROFORMING *(a)* and after the SET operation *(b)* to visualize all broken cells (see Fig. 11–*(c)*) in its 4 kbit memory array. The RRAM cell with "coordinates" (0, 0) is shown in the top left corner of the matrices. The bottom right corner of the matrices corresponds to the RRAM cell with coordinates (63, 63). In all matrices displayed in the rest of this work the cells are placed in this order.

Most of the cells in Fig. 11–*(a)* are marked blue; they are in HRS

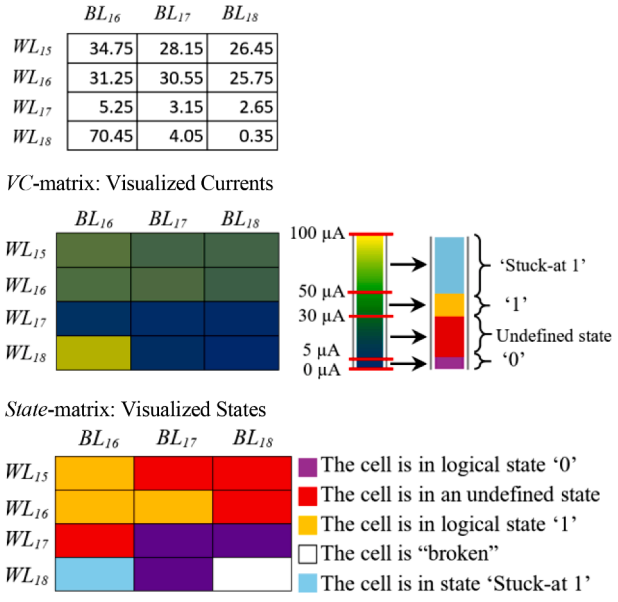


Fig. 10. Part of the RRAM chip matrices. *MC*-matrix: currents in [μA] measured after data storing, *VC*-matrix: Visualized Currents, *State*-matrix: Visualized States.

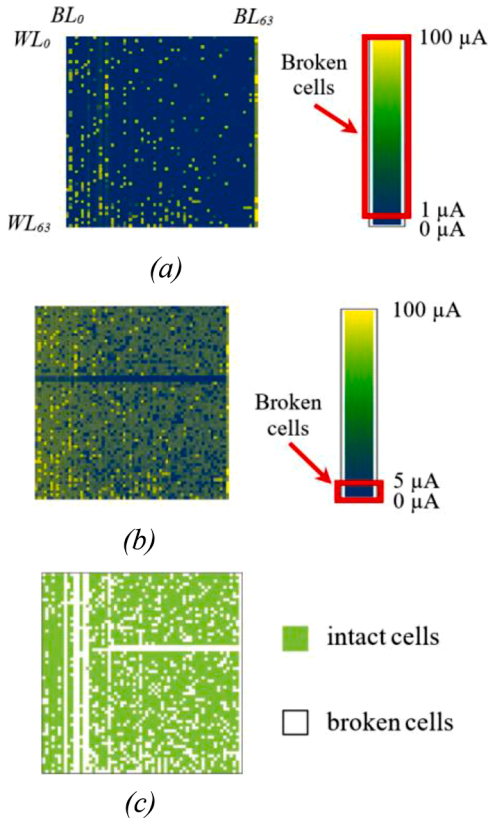


Fig. 11. The visualized matrices of the 4 kbit RRAM cells array in chip #6: *(a)* – the *VC*-matrix before ELECTROFORMING; *(b)* – the *VC*-matrix after ELECTROFORMING; *(c)* – the matrix that visualizes the broken cells.

before the ELECTROFORMING, i.e. they are intact. The cells with I > 1 μA before ELECTROFORMING are broken; they are marked yellow, blue and green. The cells that are in HRS with $I < 5$ μA after the ELECTROFORMING are also broken; they are marked blue in Fig. 11–*(b)*. The matrix in Fig. 11–*(c)* shows all these broken cells marked white. The green cells correspond to intact cells; only for these cells we evaluated the results of our laser FI experiments.

3. Impact of the READ operation on an IHP RRAM cell state

It is known that the state of RRAM cells depends on environmental parameters, e.g. on fluctuation of operating voltages/temperature or the number of performed operations [30]:

- In average the stability of the cells is high and slightly varies up to 3 μA in 10^5 cycles for SET and RESET operations.
- When the chip is exposed to temperature of 144 ℃ for a long time the conductivity of the cells in HRS is changing and this influences the resistance ratio between the cells in LRS and the cells in HRS [30].

Due to this sensitivity and taking into account the high inter-cell variability it can be assumed that the stability of an RRAM cell's state depends also on the type and/or the number of the performed operations. In the literature, we did not find any information about this possible dependability but this information is necessary for a fair evaluation of our optical FI experiments with RRAM structures. The most performed operation is the READ. Thus, at first, we performed some experiments with the goal to investigate the possible impact of the READ operation on the stability of the cell's state. The possible impact, if it can be observed, has to be taken into account when analysing the sensitivity of RRAM cells to optical fault injections.

To evaluate the impact of the READ operation on an RRAM cell's

state stability the current through the 4 kbit memory structure was measured repeatedly many times (i.e. we performed the READ operation repeatedly) and analysed the result of the READ operation – the *MC*-matrices – using statistical methods.

We assumed that the influence of the READ operation on the state of the cells is:

- insignificant;
- may depend on the cell states or on the examined chip;
- may be cumulative.

Due to these assumptions we analyzed statistically not only the whole chips but also their cell groups in the same programmed logical state. The broken cells were excluded from this analysis.

We experimented with two 4 kbit RRAM chips:

- chip #6. It was a new chip; we performed the READ operation 3 times before ELECTROFORMING and 9 times after storing the data;
- chip #2. It was a chip after performing the laser fault injection experiments; we performed the READ operation 16 times.

The chips #2 and #6 were taken in order to assess the stability of I values between READ operations for a new chip and for a chip that had already been exposed to the laser. The chips were selected for the experiments randomly from a set of the manufactured chips that exhibits moderate performance, i.e. the investigated chips here are not the top quality ones.

In order to determine the success of our FI attacks we decided to set a criterion $\boldsymbol{K}$ of *observable laser influence* based on the interval $[\overline{m} \pm 3\sigma]$, where $\overline{m}$ is the mean change of the current through all evaluated cells calculated using two *MC*-matrices and σ is the standard deviation.

We calculated $\overline{m}$ and σ for different pairs of *MC*-matrices for the chip #6 and for the chip #2. All calculated $\overline{m}$ differ slightly from 0. Due to this fact, we selected for each chip the largest calculated interval $[\overline{m} \pm 3\sigma]$, and we set the criterion $\boldsymbol{K}$ of the *observable laser influence* as:

$$K : |\Delta I| \; > \; \max\{|\overline{m} \pm 3\sigma|\} \tag{1}$$

The criterion $\boldsymbol{K}$ means:

- If the current measured through the cell before and after the laser irradiation changes more than $\max\{|\overline{m} - 3\sigma|, \; |\overline{m} + 3\sigma|\}$, it will be considered as an *observable laser influence*.
- If this change of the current causes the change of the logical state of the cell it will be considered further as a *successful FI*.

The calculated values are slightly different for both analysed chips:

- $\max\{|\overline{m} \pm 3\sigma|\} = 4.351$ μA for the chip #6;
- $\max\{|\overline{m} \pm 3\sigma|\} = 4.296$ μA for the chip #2.

One of the reasons of this difference can be the fact that the chip #2 was already irradiated with a laser, opposite to the chip #6. Another reasons can be the device-to-device variability and the fact that these chips were taken from different wafers. Since all other chips attacked in this work were taken from the same wafer as the chip #2 (see section *V*) we assign the criterion $\boldsymbol{K}$ to the value of 4.296 μA that we obtained for chip #2. The value of criterion $\boldsymbol{K}$ is important due to its influence on evaluation of the attack results.

4. Setup and first laser FI Experiments

The goal of our experiments is to investigate the sensitivity of IHP RRAM cells to optical FIs attacks. Due to the known sensitivity of the MIM structures to heating [30] we expected that laser irradiation, especially infrared laser, can influence on the logic state of the RRAM cells or at least can influence the value of the current through the MIM structure without changing the logic state of the cell.

According to the process of the conductive filament formation/rupture we assume that the illumination of the MIM structure(s) leads possibly to additional creation/recombination of the Frenkel pairs at the $Ti/Al:HfO_2$ interface, especially if the laser beam hits the MIM structure. This creation/recombination of the Frenkel pairs leads to thickening/thinning or formation/rupture of the conductive filament that influences the conductivity of the MIM structure. It is not known which process – the formation or the rupture of the conductive filament – will be triggered when the laser illuminates/hits the MIM structure.

We assume that the influence of the laser can be "cumulative", i.e. that not only the intensity of the light pulse and its duration but also the number of the light pulses can influence the state of the attacked RRAM cell.

The equipment we used in our experiments is described in the next subsection.

4.1. Fault Injection Setup

Our optical Fault Injection setup is shown in Fig. 12.
It consists of:

- A PC with the Riscure Inspector FI software. It allows to create a so-called "FI program". An FI Program allows to store the applied set of parameters in an experiment, i.e. the power of the laser beam, the pulse duration, number of pulses, etc. The saved FI program allows to repeat the experiments.
- A Riscure VC glitcher. This device is the block that generates faults (see the block in Fig. 12 placed between the block PC and the block Laser).
- The Laser. It generates light pulses corresponding to the set of parameters saved as an FI Program.
- The optical system. It allows to focus the beam and reduce the spot size to micrometre units.
- An X-Y stage. It allows to move the attacked chip and perform scanning.

The PC is connected with an X-Y stage, a microscope camera and a

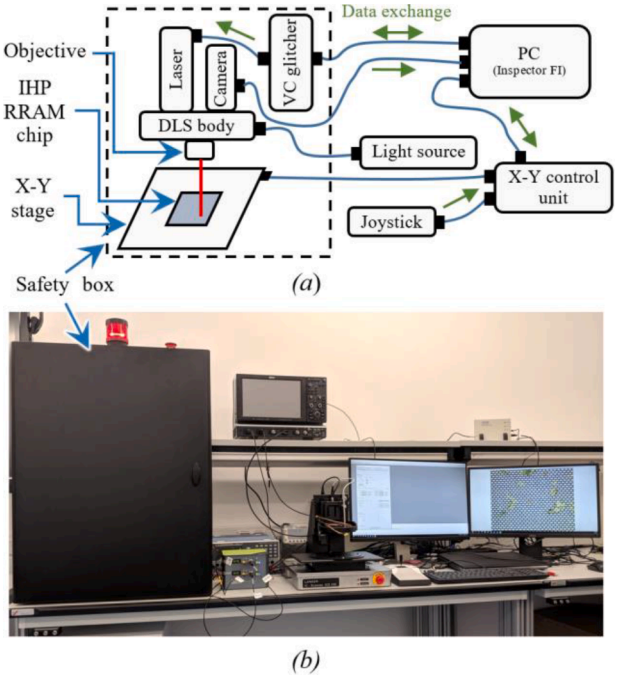


Fig. 12. Fault Injection setup: *(a)* – schematic view; *(b)* – setup at IHP.

VC glitcher via USB ports. The VC glitcher in turn is connected with a Laser via a cable with SMA connectors. All blocks except the PC, the light source and the X-Y control unit with the joystick are placed into a Safety box. It protects the user from the potentially harmful reflections of the laser beam.

We used in our experiments the 1st generation Riscure Diode Laser Station (DLS) [31]. **Fig. 13** shows the Diode Laser Station as a part of the laboratory equipment at IHP. Corresponding to the Riscure data sheet [31] the parameters of the DLS are:

- The DLS is equipped with two multimode laser sources:
  - 14 W for the red laser 808 nm;
  - 20 W for the near infrared (NIR) laser 1064 nm;
- pulse duration in a range of 20 ns – 100 μs;
- trigger delay is 50 ns;
- elliptical spot sizes 60×14 μm^2, 15×3.5 μm^2, 6×1.5 μm^2 or 3×0.8 μm^2 (expected spot size where 80 % of the power is concentrated);
- magnification objectives: 5×, 20×, 50×, 100×;
- Filters: 10%, 1%, 0.1%;
- X-Y stage with 3 μm accuracy and 0.05 μm [31] step distance between two adjacent points.

Usually the near-infrared laser source is used to perform experiments through the back-side of the attacked chip due to the fact that the substrate is transparent to the infrared spectrum [32].We begin with front-side attacks using the red laser, but we assume that using a near-infrared laser will be more effective. We start with the red laser because it has lower power at the output of the laser system[8], i.e. lower probability to destroy the chip.

Due to the laser that we selected for our first FI experiments the parameters of the laser source/beam are:

- Time:

The lasers used in the DLS are operated only in a pulse mode.

- Optical filter:

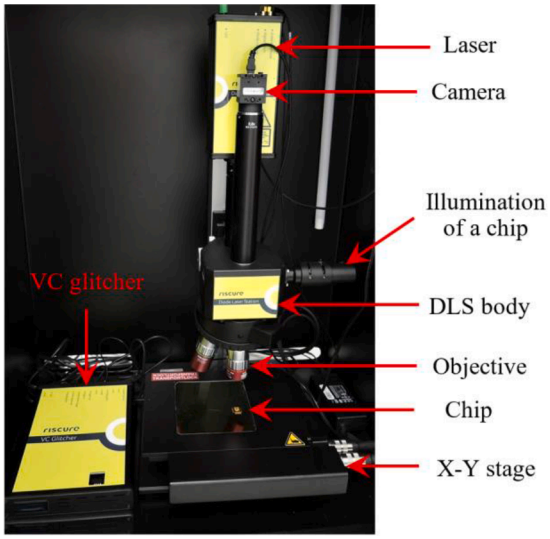


Fig. 13. Riscure Diode Laser Station and VC glitcher (see yellow box at the left side of the picture).

The optical filter in the system is used to reduce the output power of the laser. We reduced the output power in the beginning in order to lower the probability of damaging the chip by the laser beam.

- Spot size of the laser beam:

The size of the spot depends not only on the used filter but also on the used objective. The use of the higher magnification objective leads to smaller spot size and to the reduction of the output power of the laser system. This is due to the fact that higher magnification objective has more lenses inside and each of the lenses causes a loss of the beam energy. The smallest spot size with the used equipment is still larger than one RRAM cell and the distance between two neighbouring RRAM cells. Thus the laser illuminates/hits more than one RRAM cell simultaneously.

The success of FI depends on:

- duration of the laser pulse;
- size of the laser spot;
- power distribution in the spot;
- sensitivity of the attacked part of the RRAM structure.

Riscure did not provide us any information on:

- the spatial distribution of the energy in the laser spot;
- the exact spot size[9].

If we programmed the step distance equal to 0.2 μm or less we observed some mismatches between the number of steps programmed using the Riscure Inspector FI software and the number of steps done when observing through the microscope camera. So, we performed some measurements to verify the step size given in the Riscure datasheet. The reported one is 0.05 μm that is 50 nm or 1/5 of the IHP transistors gate length. The result of our measurements is the minimal reasonable step distance between two neighbouring points is 0.25 μm.

4.2. *VC glitcher*

To control the optical pulses of the DLS a Riscure VC glitcher [33] is used. An FI program with a configured set of parameters for FI experiments is created by the user. First VC glitcher loads an FI program on the internal Field-Programmable Gate Array (FPGA). After processing of a loaded FI program VC glitcher performs scanning with the configured parameters. The VC glitcher is operated by the special software called Inspector FI [34].

4.3. *Inspector Fault Injection software*

The Inspector FI software allows to control not only the power and duration of the laser pulse but a programmable X-Y stage, i.e. to create an FI program. **Fig. 14** shows the Inspector FI application window with a tab to configure the X-Y stage and a part of the attacked RRAM chip.

To perform laser FI experiment the user has to select a perturbation window. It contains 8 tabs to create an FI program.

In the following subsection we describe the configuration of the X-Y stage in our experiments.

4.4. *Moving the attacked chip in our experiments*

The goal of our first experiments was to define the parameters of the laser set-up for a successful and repeatable *observable laser influence* without any previous knowledge about the sensitivity zones in RRAM

[8] Laser system consists of: laser, spot size reducer, DLS body and magnification objectives.

[9] The sizes given in laser data sheet [31] with the use of objectives show the spot sizes where 80% of the energy is concentrated.

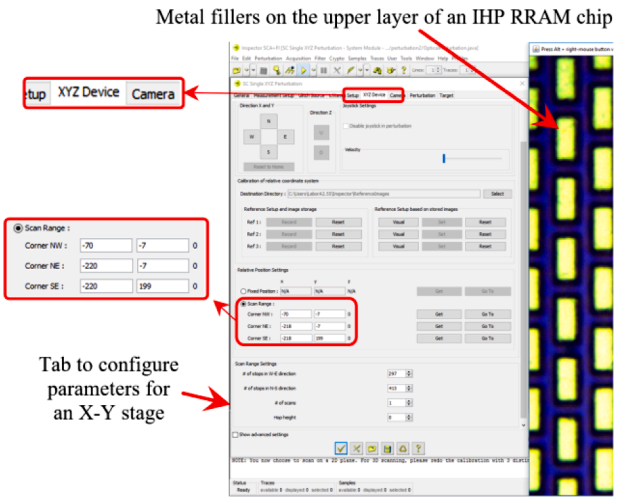


Fig. 14. The windows of the Inspector FI software.

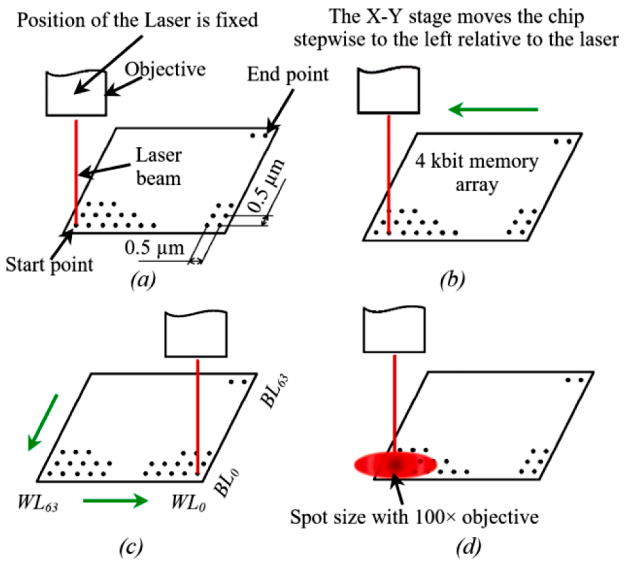


Fig. 15. Position of the attacked chip placed on the programmed X-Y stage: *(a)* – 1st (start) point in the 1st *X*-movement line corresponds to the cell (WL_{63}; BL_0); *(b)* – 2nd point in the 1st *X*-movement line is the cell (WL_{62}; BL_0); *(c)* – last point in the 1st *X*-movement line is the cell (WL_0; BL_0); *(d)* – 1st point of the 2nd *X*-movement line is the cell (WL_{63}; BL_1). The distance between two adjacent points in each *X*-movement line is 0.5 µm for the X axis; the distance between two neighbour *Y*-movement lines is 0.5 µm for the Y axis. After the first X-movement line is scanned the table moves to the start point of the scanned X line, and after it moves along the Y axis to the next X-movement line.

structures. In our experimental set-up no voltages can be applied to the cells of the attacked RRAM chip, i.e. injecting faults into the NMOS transistor is not possible. So we are focusing on injecting faults in the memristor.

We scanned the whole 4 kbit memory array because the IHP technology requires implementing metal fillers in manufactured chips. The metal fillers are relatively small metal areas that are placed in different metal layers between the wires to maintain the chip's stiffness during its manufacturing. Fig. 14 shows a part of the investigated RRAM chip through the microscope camera with a 100× magnification objective. The yellow rectangles in Fig. 14 are the metal fillers. Thus, the wires inside the chip and metal fillers are obstacles to the laser beam and can reduce the success of the *observable laser influence*. Due to these facts we scanned the whole area of this RRAM array.

We performed many chip scans applying different laser set-up parameters. We started with the minimal laser pulse duration and low energy to avoid harming the analyzed chip.

The position of the Laser is fixed in the Riscure setup. So, the attacked chip has to be moved to illuminate its different parts. The active movement is performed by an X-Y stage manufactured by Märzhäuser Wetzlar GmbH & Co [35]. The range and the minimal distance of movements are corresponding to our measurements as follows:

- Along the X axis the range of movement is 75 mm with a minimum possible distance between two adjacent points of 0.25 µm;
- Along the Y axis the range of movement is 50 mm with a minimum possible distance between two adjacent points of 0.25 µm.

We programmed the movement of the stage using the Riscure Inspector FI Software. The area occupied by the 4 kbit memory array is 146×204 µm^2, see Fig. 6–*(a)*. We set the area for the scan to 148×206 µm^2, i.e. we added 1 µm in each direction to the area of the attacked chip due to the possible inaccuracy of the chip placement on the X-Y stage surface, e.g. the chip can be placed at a slight angle as well as to the possible step inaccuracy caused by the X-Y table.

In our experiments we set the distance of 0.5 µm between two adjacent points due to the area occupied by one MIM structure, i.e. 0.6×0.6 µm^2 in the tested IHP RRAM chip. This guarantees at least one hit of the center of the laser spot on the MIM structure. Fig. 15 shows the position of the stage in our experiments with the selected step distance between two neighbouring points.

Due to the selected step distance between two neighbouring points, the size of the RRAM cell (2.2×3 µm^2) and the area of the laser beam spot a different number of the RRAM cells can be illuminated/hit by one laser shot.

5. Preparation of the chip for FI experiments

We performed scans with three new 4 kbit RRAM chips in total. The targeted chips are marked with numbers #2, #4 and #9. The acquired 4 kbit RRAM chips were in packages that we opened, see section *II-D*, Fig. 8–*(b)*.

5.1. Programming of the 4 kbit RRAM chips

The cells in these chips were programmed to different logical states. This was done in order to assess how the laser influences the cells in different states.

Chip #4 and **Chip #9**

After the ELECTROFORMING the chip #4 and the chip #9 were programmed to the logical states '1' and '0' as follows:

- cells with *Word Lines* 0-15 – block 1 – were programmed to the logical state '0'.
- cells with *Word Lines* 16-31 – block 2 – were programmed to the logical '1'.
- cells with *Word Lines* 32-47 – block 3 – were programmed to the logical '0'.
- cells with *Word Lines* 48-63 – block 4 – were programmed to the logical '1'.

Fig. 16 shows the visualized matrices of the chip #4 before ELECTROFORMING (see Fig. 16–*(a)*) and after data storing (see Fig. 16–*(b)*, *(c)*).

Storing the data in the chip #4 was performed without any failures. The chip #4 showed a good distribution in *I* values after storing the data, i.e. almost all the cells were successfully programmed, see Fig. 16–*(b)*. Only 62 RRAM cells are in an undefined state, see red points in Fig. 16–*(c)*. But there are still 499 broken cells, see white points in Fig. 16–*(c)*. So, there are 1765 cells in state '0' and 1770 cells in state '1'.

Fig. 17 shows the visualized matrices of the chip #9 before

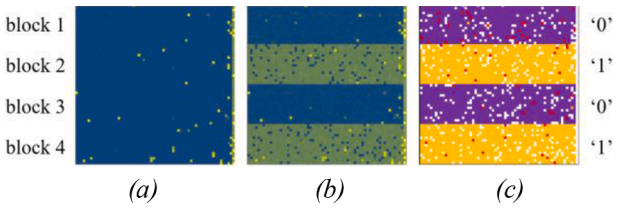


Fig. 16. The visualized matrices of the 4 kbit memory array of the chip #4: *(a)* – the *VC*-matrix before ELECTROFORMING; *(b)* – the *VC*-matrix after storing the data; *(c)* – the *State*-matrix after storing the data.

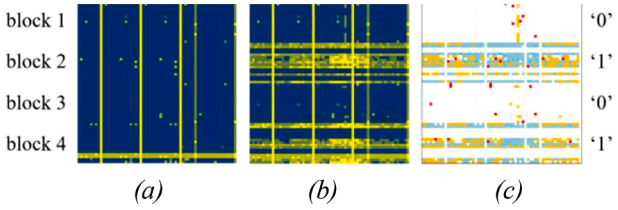


Fig. 17. The visualized matrices of the 4 kbit memory array of the chip #9: *(a)* – the *VC*-matrix before ELECTROFORMING; *(b)* – the *VC*-matrix after storing the data; *(c)* – the *State*-matrix after storing the data.

ELECTROFORMING (see Fig. 17–*(a)*) and after data storing (see Fig. 17–*(b),(c)*).

The chip #9 was the worst sample in terms of reliability in our experiments. There are 509 cells identified as broken before ELECTROFORMING, see yellow points in Fig. 17–*(a)*. The *MC*-matrix after storing the data (see Fig. 17–*(b)*) shows that many cells in blocks 1 and 3 are in logical state '0' as they were programmed. However due to the absence of the *MC*-matrix after ELECTROFORMING we do not know if the cells (marked in white) in blocks 1 and 3 were successfully ELECTROFORMed or not. Hence we consider these cells as broken according to the definition in section *II-C*. The number of broken cells after storing the data is significant and equals to 3100 RRAM cells, see cells marked in white in Fig. 17–*(c)*. Though there are only 27 RRAM cells in an undefined state, i.e. there are only 376 cells in state '1' and 593 cells in the 'Stuck-at 1' state.

Chip #2

After the ELECTROFORMING of the chip #2 the logical state '1' was stored in each cell of the entire 4 kbit memory array, i.e. the operations were performed in the following sequence: ELECTROFORMING → RESET → SET. Fig. 18 shows the visualized matrices of the chip #2 before ELECTROFORMING (see Fig. 18–*(a)*) and after storing the data (see Fig. 18–*(b), (c)*).

159 cells of the chip #2 were identified as broken before ELECTROFORMING. The number of the cells in the undefined state after storing the data into chip #2 is 530. In addition the chip #2 has 1230 cells in the 'Stuck-at 1' state. This may be explained as follows: the chip #2 had failures when storing the data. Particularly, when storing the logical state '1' into the 2 *Word Lines* (WL_0, WL_1) the result of the performed READ operation, i.e. *MC*-matrix showed changes in the 6 *Word Lines* (from WL_0 to WL_6). We assume that this happened due to failures when addressing the *Word Lines* or the pins were in short circuit state during characterization process. As result chip #2 has only 1383 cells in state '1'.

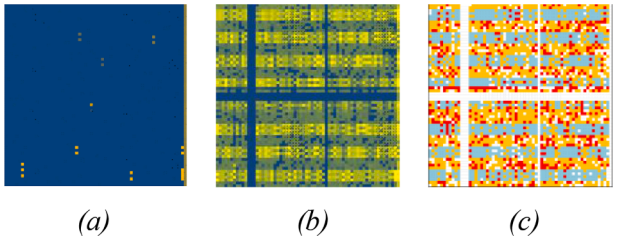


Fig. 18. The visualized matrices of the 4 kbit memory array of chip #2: *(a)* – the *VC*-matrix before ELECTROFORMING; *(b)* – the *VC*-matrix after storing the data; *(c)* – the *State*-matrix after storing the data.

After the storing the data we placed the targeted and opened chip on the X-Y stage as shown in Fig. 19.

In the next section we describe our optical FI experiments and discuss their results.

6. Results of our laser FI experiments

We denote a laser scan of the 4 kbit RRAM memory array performed using a certain set of parameters as an experiment. Not all experiments that we performed were done in the automated mode. In many experiments the pulse duration and number of shots per move were adjusted manually, see TABLE II – TABLE IV. The automated mode is limited by a maximum pulse duration of 100 µs but it allows to program the X-Y stage and to perform the scanning of the attacked chip automatically, always with the same – programmed and stored – parameters: laser beam output power, pulse duration, movement distance, shots per move, etc. In the manual mode the X-Y positioning stage is controlled manually using a joystick (manipulator), see Fig. 12. This mode allows to bypass the limitation of the 100 µs for the maximum pulse duration, but every shot should be performed manually. The pulse durations we applied in our experiments were calculated for the "Glitch Source" tab in "SC Single XYZ Perturbation" menu. Due to the longer pulse duration than in automated mode there is a high probability that the surface of the chip or the chip itself may be damaged, e.g. RRAM cells, decoders, operation control circuit, see subsection *II-D*. For this reason each of the three attacked IHP RRAM chips was scanned in the automated mode, first. Experiments done in manual mode are marked with grey background in TABLE II – TABLE IV.

We started our attacks with the chip #2. First we performed the READ operation. The measured currents were stored as the matrix $MC_0^{\#2}$. Then we performed the first laser scan with the following parameters:

- 50% laser beam power;
- 20 ns pulse duration;
- 10% optical filter;
- 1 laser shot per move;
- 0.5 µm distance between two adjacent cells for both X- and Y-axis;
- 100× magnification objective.

After the scan we performed the READ operation again and stored the measured currents as matrix $MC_1^{\#2}$. To evaluate the success of the FIs in the experiment we calculate the difference of the matrices $\Delta_{1,0}^{\#2} = MC_1^{\#2} - MC_0^{\#2}$ and analyzed it. If a value $\delta_{j,i}^{\#2} \in \Delta_{1,0}^{\#2}$, i.e. the change of the current through the cell with the coordinates (WL_j, BL_i), is larger than 4.296 µA ($|\delta_{j,i}^{\#2}| \geq 4.296$ µA), we consider it as an *observable laser influence*, see criterion ***K*** in section III. Thus for each value $|\delta_{j,i}^{\#2}| \geq 4.296$ µA in the Δ-matrix we check the logical state of the cell with the coordinates

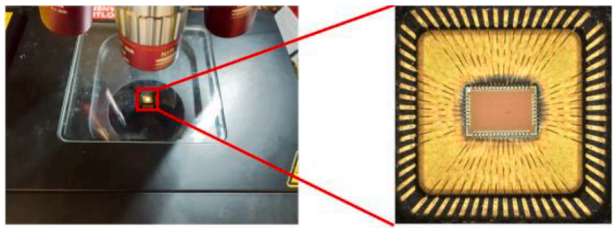


Fig. 19. Placement of the opened chip on the X-Y stage.

(WL_j, BL_i) before and after the performed laser scan in order to detect successful FIs. Please note that we excluded 953 RRAM cells in chip #2 from our analysis since they were determined as broken. TABLE I shows the results of the 1st FI experiment.

Fig. 20 shows a matrix that visualizes the successful FIs in RRAM cells after the 1st experiment with the chip #2. The color legends in TABLE I and **Fig. 20** are the same.

In the following experiments we increased the power, the pulse duration, the number of shots per move and applied different objectives. The parameter set for each experiment is given in TABLE II – TABLE IV. After each experiment l we performed the READ operation, stored the matrix of measured currents $MC_l^{\#2}$, and evaluated the success of the FIs calculating the difference matrix $\Delta_{ll-1}^{\#2} = MC_l^{\#2} - MC_{l-1}^{\#2}$ applying the threshold $|\delta_{i,j}^{\#2}| \geq 4.296$ μA as the criterion $\boldsymbol{K}$ of a measurable *observable laser influence*.

We performed similar experiments and analysis for the chips #4 and #9. TABLE II – TABLE IV give an overview of these experiments.[10]

Please note that the values of measured currents $I_{j,i}$ for the cell (WL_j, BL_i) for any two READ operations are always slightly different. Due to this fact for some cells their logical state can change even without laser illumination (but only for undefined state ↔ '1', undefined state ↔ '0' or 'Stuck-at 1' ↔ '1' are possible). In TABLE II – TABLE IV we give the results of our experiments for the observed laser influences and the logical state changes (transitions). Please note that the transitions cannot be directly calculated from the columns giving the numbers per state and chip before scan and after scan.

TABLE V gives an overview of all laser influences observed in our experiments.

The number of influenced cells is significantly higher for attacks performed in manual mode, except for chip #2.

Fig. 21 shows the total number of influenced RRAM cells for each chip in all experiments done, i.e. it represents the data given in TABLE II – TABLE IV graphically.

Experiments carried out show that the reaction of the attacked chips to laser irradiation is different. Nevertheless, it is clear the cells in LRS, i. e. in logical state '1' and in 'Stuck-at 1' state, are prone to laser influence.

Table I
Overview of the successful laser influences for the 1st laser scan experiment with the chip #2[a, b, c]

Successful FI (change of cell's state)												Not FI		
'0'→undef.	'0'→'1'	'0'→ Stuck-at 1	undef.→'0'	undef.→'1'	undef.→ Stuck-at 1	'1'→'0'	'1'→undef.	'1'→ Stuck-at 1	Stuck-at 1 → '0'	Stuck-at 1 → undef.	Stuck-at 1 → '1'	Changed state[b]	Observable laser influence[c]	Uninfluenced cells
0	0	0	31	11	0	8	9	0	0	12	104	148	66	2754

[a] There are 953 cells from 4096 cells broken, they were excluded from the experiments.
[b] The cells that changed their state without observable laser influence.
[c] The cells that were successfully influenced but without changing their state.

[10] Manual mode: in this mode not the whole RRAM chip was attacked, but some selected areas. These areas were selected randomly and differ for each objective. The areas do not overlap. The amount of shots per position varied from 1-5 because it was not possible to define this number precisely due to the manual mode.

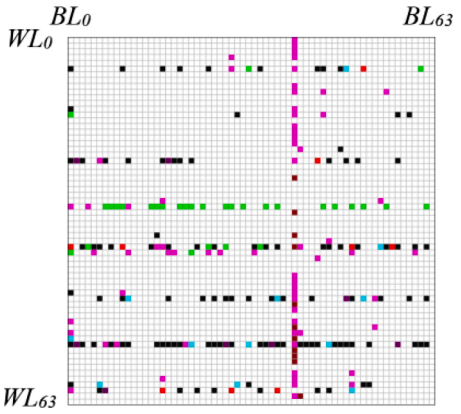


Fig. 20. Visualized matrix of successful laser influences of the 1st experiment with the chip #2.

This can be clearly seen from the experiments with chip #2 performed in automated mode and experiments performed with chip #4 and chip #9 in manual mode. However, due to the small number of experiments performed, i.e. lack of data, an appropriate generalization is infeasible. Hence, we describe the laser influence on each chip individually.

Chip #2, see TABLE II:

The surface of the chip #2 was damaged after the experiments in manual mode, i.e. it shows visible traces of the laser irradiation. However, the internal structure of the chip was not damaged. Chip #2 is still fully functional after all experiments performed, i.e. it still responds to the READ operation without any failures.

Most of the experiments with chip #2 were performed in the automated mode. The following transitions are dominating:

- 149 transitions from logical state '1' to the state 'Stuck-at 1' in the automated mode;
- 131 transition from 'Stuck-at 1' state to the logical state '1', of which 109 transitions happened when running experiments in the automated mode.

We observed a lot of cells that were successfully influenced but did not change their state. The following influences were observed:

- 107 influences in cells in the logical state '1', of which 105 influences were observed when experiments were run in the automated mode;
- 118 influences in cells in 'Stuck-at 1' state, of which 114 were observed when experiments were run in the automated mode.

Thus, for chip #2 we can conclude that RRAM cells that are in LRS, i. e. in logical state '1' and in the 'Stuck-at 1' state, are sensitive to laser influence. This observation is biased by the fact that chip #2 was programmed to LRS only. We cannot exclude that the cells in logical state '0' are even more sensitive to laser irradiation, due to the fact that the very small number of cells in logical state '0' that we observed in our experiments changed their state spontaneously:

- 18 of 49 cells in state '0' in experiment 2,
- 5 of 20 cells in state '0' in experiment 3,
- 15 of 16 cells in state '0' in experiment 4.

According to TABLE II, we can conclude that the success of FIs for chip #2 in automated mode is more likely with a low laser beam power and a short pulse duration. But the number of experiments performed in manual mode, i.e. with high power and long pulses is too small to draw conclusions on the effect caused by these parameter settings.

Chip #4,see TABLE III:

Chip #4 was damaged during the experiments. The surface of the

Table II
Overview of laser scan experiments with chip #2[d]

Laser scan experiment	Parameters of the laser station				chip #2 before scan				chip #2 after scan				Laser influence FI			
	Power, %	Pulse durarotion, ns	Objective	Shots per position	'0'	'1'	Undefined state	Stuck-at 1	'0'	'1'	Undefined state	Stuck-at 1	'0'→ undefined	'0'→ '1'	'0'→Stuck-at 1	undefined→'0'
1*	50	20	100×	1	0	1383	530	1230	49	1477	503	1114	0	0	0	31
2	70	20	100×	1	49	1477	503	1114	20	1371	552	1200	9	9	0	0
3	100	100	100×	1	20	1371	552	1200	16	1365	533	1229	5	0	0	0
4	100	10^5	100×	1	16	1365	533	1229	0	1348	506	1289	1	3	11	0
5	100	10^5	50×	1	0	1348	506	1289	2	1363	493	1285	0	0	0	0
6	100	10^5	20×	3	2	1363	493	1285	2	1376	467	1298	0	0	0	0
7	100	10^5	5×	3	2	1376	467	1298	2	1374	461	1306	0	0	0	0
8	100	$5{\cdot}10^6$	100×	1-5	2	1374	461	1306	2	1373	462	1306	0	0	0	0
9^{10}			20×		2	1373	462	1306	2	1374	473	1293	0	0	0	1
10^{10}			5×		2	1374	473	1293	7	1391	493	1252	0	0	0	0

d953 from 4096 cells are broken and excluded from experiments.
*The experiment is performed with 10 % optical filter.

chip #4 was damaged after the experiments 4-6. However, the chip still showed a correct behaviour, so that we assume that its internal structure was still intact. After the experiment 9 the chip #4 stopped functioning and could not be operated anymore. Thus, we assume that changes of the cells states in the 9th experiment, see TABLE III, occurred because of the damage of the internal structure. It means that a pulse duration of 50 ms and the use of 5× magnification objective can damage not only the surface but also internal structure of the chip, see subsection *II-D*.

For chip #4 we observed the following state transitions:

- 89 from logical state '0' to an 'undefined' state, of which 19 were observed when experiments were run in the automated mode;
- 882 transitions from logical state '1' to logical state '0' in manual mode;
- 30 transitions from logical state '1' to an 'undefined' state in manual mode;
- 87 transitions from an 'undefined' state to logical state '0', of which only 2 were observed when experiments were run in the automated mode.

There are also cells that were influenced (see the criterion ***K*** for the *observable laser influence*) but did not change their state:

- 57 influenced cells in logical state '1', of which only 3 cells were influenced in the automated mode;
- 40 influenced cell in logical state '0', of which only 5 cells were influenced in the automated mode.

Hence for chip #4:

- the cells in HRS are sensitive to laser influence in the automated mode;
- the cells in LRS are sensitive to laser influence in the manual mode.

According to TABLE III, we can conclude that the success of FI for chip #4:

- in automated mode is more likely with a short pulse duration;
- in manual mode is more likely with long pulse duration and a small magnification objective.

Chip #9, see TABLE IV:

We performed only a small number of experiments with chip #9 due to the fact that it was mechanically damaged after the 3rd experiment, i.e. several bonding wires were detached from the chip pads. Nevertheless, we run experiments and observed that the following transitions are dominating in the manual mode (last experiment, i.e. before chip #9 was damaged):

- 377 transitions from logical state '1' to logical state '0';
- 598 transitions from the 'Stuck-at 1' state to logical state '0'.

In the automated mode (see experiments 1 and 2) we observed that the following influences are dominating:

- 15 influenced cells in logical state '1';
- 49 influenced cells in the 'Stuck-at 1' state.

Thus, for chip #9 we conclude that the cells in LRS are sensitive to laser influence in automated and manual modes. We admit that these results are biased by the fact that chip #9 had no cells in HRS, i.e. logical state '0'. According to TABLE IV, we can conclude that the success of FI in the automated mode for chip #9 is more likely with a low laser beam power.

Comparing the data in TABLE II – TABLE IV we can conclude that in the automated mode FIs are more successful when run with the following parameters:

- a low laser beam output power;
- a short pulse duration;
- the 100× magnification objective, i.e. with the smallest laser beam spot size in our setup.

Experiments in a manual mode show that:

- the success of FIs is more likely with a long pulse duration and small magnification objectives;
- the damage of the surface and the damage of the internal structure of the chip is also more likely with a long pulse duration and small magnification objectives.
- According to the visual inspections of the chips before and after the experiments we can conclude that in the automated mode: the configuration of the variable parameters in our experiments leads to no damage, neither to the passivation layer nor to the internal structure; in the manual mode the following parameters: 1 ms pulse duration; 100% laser beam output power; 100× magnification objective may lead to the distinct visible damage of the chip surface;
- in the manual mode a damage of the internal chip structure may occur with following parameters: 50 ms pulse duration; 100% laser beam output power; 5× magnification objective.

Main results of our experiments are:

Laser influence FI								no change in the logic state of the cells				Change of states without laser influence
undefined→'1'	undefined→Stuck–at 1	'1'→'0'	'1'→undefined	'1'→Stuck-at 1	Stuck-at 1→'0'	Stuck-at 1→undefined	Stuck-at 1→'1'	'1'→'1'	'0'→'0'	undefined→undefined	Stuck-at 1→Stuck-at 1	
11	0	8	9	0	0	12	104	27	0	12	27	148
6	10	0	10	82	0	0	3	23	1	5	23	159
2	2	0	0	22	0	0	0	5	0	5	2	137
8	22	0	1	29	0	0	0	3	0	5	4	137
7	0	0	2	2	0	0	1	16	0	5	18	143
11	0	0	0	12	0	0	1	28	0	6	32	127
2	0	0	1	2	0	0	0	3	0	0	8	145
0	0	0	0	0	0	0	0	0	0	0	0	6
1	0	0	4	0	0	0	22	1	0	5	3	83
0	0	3	3	0	2	28	0	1	0	2	1	68

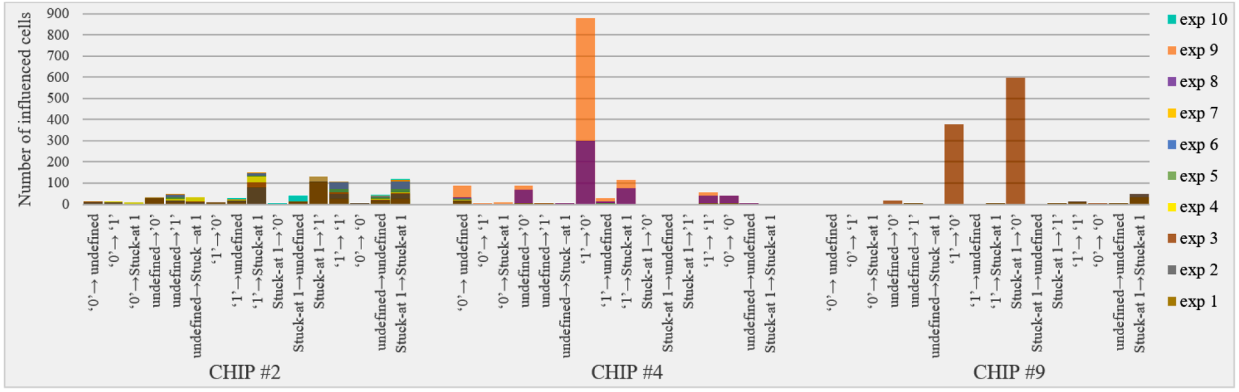
- the change of the logical states as a result of the laser influence is observable in all attacked chips;
- reaction of chips to laser illumination is individual (the most sensitive chip in our experiments is the chip #4);
- in the automated mode the first laser scan experiment has the highest number of influenced cells. The reduced number of the influenced cells in subsequent experiments can be caused by: 1) sequentially executed experiments (the cells that are easy to influence probably switched their logical state already in the previous experiment); 2) the new parameter set only.

So the sets of parameters applied in our laser experiments that caused successful FIs require additional experiments to be confirmed. Experiments with a low laser beam output power should be performed in order to confirm or disprove the higher laser influence on the cells state when using a low laser output power. But for the sake of completeness we determine the areas of the investigated RRAM chips sensitive to laser irradiation using the results presented here so far.

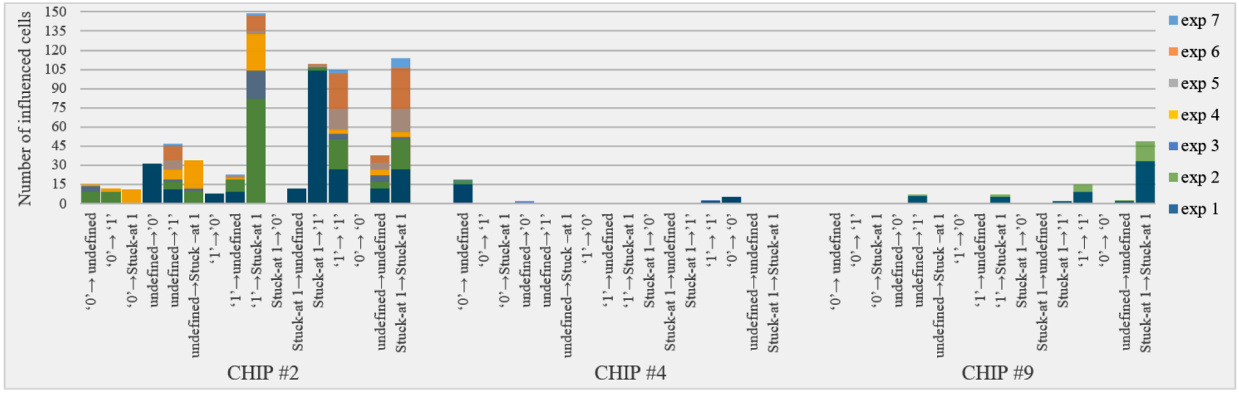
6.1. Determining RRAM chips sensitive areas

In order to determine the sensitive areas of RRAM chips we overlaid matrices of the laser influence (*ML*-matrices) for all attacked chips. We may do so as they have the same layout. Fig. 22 visualizes cells, which were influenced on each single chip and in all laser scan experiments performed.

If a cell was influenced only in one of the laser scan experiments performed, we marked the cell green and consider it as a low sensitive



(a)



(b)

Fig. 21. Total number of influenced RRAM cells for each chip in all experiments carried out in: *(a)* – automated and manual mode; *(b)* – automated mode only.

Table III
Overview of laser scan experiments with chip #4[e]

Laser scan experiment	Parameters of the laser station				chip #4 before scan				chip #4 after scan				Laser influence FI				
	Power, %	Pulse durarotion, ns	Objective	Shots per position	'0'	'1'	Undefined state	Stuck-at 1	'0'	'1'	Undefined state	Stuck-at 1	'0'→ undefined	'0'→ '1'	'0'→ Stuck-at 1	undefined →'0'	undefined →'1'
1	100	40	100×	1	1765	1770	62	0	1727	1743	127	0	15	0	0	1	0
2	100	10^4	100×	1	1727	1743	127	0	1704	1745	148	0	3	0	0	0	0
3	100	10^5	100×	3	1704	1745	148	0	1702	1756	139	0	1	0	0	1	1
4[10]	100	10^6	100×	1-5	1702	1756	139	0	1701	1756	140	0	1	0	0	0	0
5[10]			20×		1701	1756	140	0	1695	1748	154	0	4	0	0	1	0
6[10]			5×		1697	1751	159	0	1694	1741	162	0	5	0	0	2	0
7[10]	100	$5{\cdot}10^7$	100×	1-5	1694	1741	162	0	1698	1739	160	0	0	0	0	0	0
8[10]			20×		1698	1739	160	0	2056	1421	107	13	3	0	0	63	2
9[10]			5×		2056	1421	107	13	2570	709	189	129	57	1	9	19	1

e499 from 4096 cells are broken and excluded from experiments.

Table IV
Overview of laser scan experiments with chip #9[f]

Laser scan experiment	Parameters of the laser station				chip #9 before scan				chip #9 after scan				Laser influence FI			
	Power, %	Pulse durarotion, ns	Objective	Shots per position	'0'	'1'	Undefined state	Stuck-at 1	'0'	'1'	Undefined state	Stuck-at 1	'0'→ undefined	'0'→ '1'	'0'→ Stuck-at 1	undefined →'0'
1	50	20	100×	1	0	376	27	593	5	381	17	593	0	0	0	0
2	90	20	100×	1	5	381	17	593	4	377	17	598	0	0	0	0
3[10]	100	10^7	100×	1-5	4	377	17	598	996	0	0	0	0	0	0	17

f3100 from 4096 cells are broken and excluded from experiments.

cell. The cells, which were influenced in two laser scan experiments, are marked blue and considered to be moderate sensitive cells. The cells, which were influenced in 3 laser scan experiments, are considered as high sensitive cells and are marked orange. Very high sensitive cells are those cells, which were influenced in 4 laser scan experiments, they are marked red. In our experiments were no cells, which were influenced in 5 or more experiments. The broken cells as well as the cells, which did not change their state at all are marked white in **Fig. 22**.

Fig. 22 clearly shows that the positions of influenced cells in the chips are not random, i.e. the laser irradiation mostly influences cells in some *Word Lines* and in some *Bit Lines*. In case of chip #2 the periodicity of successfully attacked *Word Lines* can be seen, i.e. the cells in each seventh and/or eighth line are influenced. We expect that this is due to the fact that there are no metal fillers over the cells in each seventh/eighth *Word Line* in the IHP RRAM chips. However, in case of chip #4 and chip #9 we observed that there are a lot of cells influenced only once. These cells were in the state '1' and most of them were influenced in the last laser scan experiments, i.e. before the chips were damaged, see TABLE III – TABLE IV. The overlaid matrices of chip #4 and chip #9 neither do allow to identify especially sensitive areas nor periodicity of successfully influenced *Word Line(s)* or *Bit Line(s)*.

Fig. 23 visualizes the cells that are sensitive on all chips, or on only two chips, or even only on a single chip.

There are:

- only 35 cells were influenced in all 3 attacked chips, These cells we marked red in Fig. 23;
- In addition 645 cells were influenced on two out of the three chips, i.e. either in chip #2 and in chip #4, or in chip #2 and in chip #9, or in chip #4 and in chip #9. These cells are marked orange in Fig. 23;
- 1334 cells were influenced only on one of the three attacked chips, i.e. only in chip #2, or only in chip #4, or only in chip #9. These cells are marked grey in Fig. 23.

To verify our assumption that metal fillers may be a suitable means to prevent FI from being successful we checked their position in the attacked RRAM chips by an optical inspection using our Scanning Electron Microscope (SEM). The RRAM chip was prepared for the SEM-imaging using a Focus Ion Beam (FIB) cut in an IHP laboratory. We selected the area for the cross section using results of the optical FI attacks performed and RRAM chip layout. **Fig. 24** shows a part of the attacked RRAM chip surface that was captured using a 100× magnification objective *(a)* and a cross section image of the chip that was made with our Scanning Electron Microscope *(b)*.

The metal fillers in the attacked chips have similar width and length but different thickness according to the technological process. They are placed exactly under each other in Top Metal 1 and Top Metal 2. Thus, there are "gaps" between metal fillers through which the laser beam can freely propagate and irradiate the cell. Since we attacked standalone RRAM chips the laser irradiation influenced the MIM structure in RRAM cell. The placement of the metal fillers in Top Metal 1 and Top Metal 2 leads to the fact that they do not cover all MIM structures in RRAM chips, see cells marked by dashed grey rectangles in **Fig. 24**–*(b)*. **Fig. 25** shows the so marked areas zoomed in.

We distinguish three different cases:

- a MIM structure, which is fully covered by metal fillers, see Fig. 25–(a);
- a MIM structure, which is not covered by metal fillers, see Fig. 25–(b);
- a MIM structure, which is partially covered by metal fillers, see Fig. 25–(c).

Laser influence FI							no change in the logic state of the cells				Change of states without laser influence
undefined→Stuck–at 1	'1'→'0'	'1'→undefined	'1'→Stuck-at 1	Stuck-at 1→'0'	Stuck-at 1→undefined	Stuck-at 1→'1'	'1'→'1'	'0'→'0'	undefined→undefined	Stuck-at 1→Stuck-at 1	
0	0	0	0	0	0	0	2	5	0	0	121
0	0	0	0	0	0	0	0	0	0	0	134
0	0	0	0	0	0	0	1	0	0	0	126
0	0	0	0	0	0	0	0	0	0	0	6
0	0	1	0	0	0	0	1	0	0	0	58
0	0	0	0	0	0	0	1	0	0	0	69
0	0	0	0	0	0	0	0	0	0	0	7
3	298	13	75	0	0	0	37	35	1	0	14
1	584	16	41	0	0	0	15	0	4	0	58

Laser influence FI								no change in the logic state of the cells				Change of states without laser influence
undefined→'1'	undefined→Stuck–at 1	'1'→'0'	'1'→undefined	'1'→Stuck-at 1	Stuck-at 1→'0'	Stuck-at 1→undefined	Stuck-at 1→'1'	'1'→'1'	'0'→'0'	undefined→undefined	Stuck-at 1→Stuck-at 1	
6	0	0	0	5	0	0	2	9	0	2	33	15
1	0	0	0	2	0	0	0	6	0	1	16	8
0	0	377	0	0	598	0	0	0	1	0	0	0

According to this partitioning each RRAM chip attacked here has the following number of MIM structures:

- 1824 MIM structures fully covered by metal fillers;
- 1704 MIM structures not covered by metal fillers;
- 568 MIM structures partially covered by metal fillers.

As the placement of the fillers caused a kind of "gaps" through which the laser beam can reach a MIM structure, see Fig. 24–*(b)*, we expected that laser irradiation influences the MIM structures that are not covered or only partially covered, i.e. the MIM structures underneath the "gaps". The kind of coverage of the MIM structures – fully covered, partially covered, not covered – can cause different reaction of cells to laser irradiation in the automated as well as in the manual mode. For example, due to the long duration of the laser pulses in the manual mode, a metal filler over a cell can be heated up and then can act as heat source placed close to a MIM structure. The laser irradiation with the same parameters on a not covered cell may probably damage the irradiated cell.

To verify the effect of the metal fillers on the FI we compared the matrix representing the influenced cells for each chip with the placement of metal fillers in the chip layout. Fig. 26 shows the positions of the influenced cells in the attacked chips in all experiments done.

Fig. 26 visualizes for each attacked chip the uncovered, partially covered and covered MIM structures, which were successfully influenced.

Now we describe our main observations for each chip individually.

Chip #2:

- The cells in the most influenced Word Lines WL_{29} and WL_{36} in manual and in automated modes are not covered by metal fillers, i.e. have "gaps" atop.
- The cells in the most influenced Bit Line BL_{39} in automated mode have "gaps" atop. The majority of influenced cells are partially covered by metal fillers.

Chip #4:

- In automated mode, MIM structures of all coverage types are successfully influenced, whereby the mostly influenced cells were the cells covered by metal fillers.
- In manual mode, MIM structures of all coverage types are successfully influenced regardless existence of "gaps" atop the cell.

Chip #9:

- In automated mode, all types of MIM structure coverage are successfully influenced, whereby the mostly influenced cells were the cells with MIM structures covered by metal fillers.
- In manual mode, all types of MIM structure coverage are successfully influenced regardless existence of "gaps" atop the cell.

TABLE VI shows the number of analysed cells, influenced cells and the number of *observable laser influences* in our experiments for each

Table V
Number of *laser influences* observed in our experiments.

Number of analysed cells (without the broken cells)		Chip #2 3143	Chip #4 3597	Chip #9 996
Number of *observable laser influences*	Laser scan experiments in automated mode	709	30	83
	Laser scan experiments in manual mode	77	1294	993
	All laser scan experiments	786	1324	1076

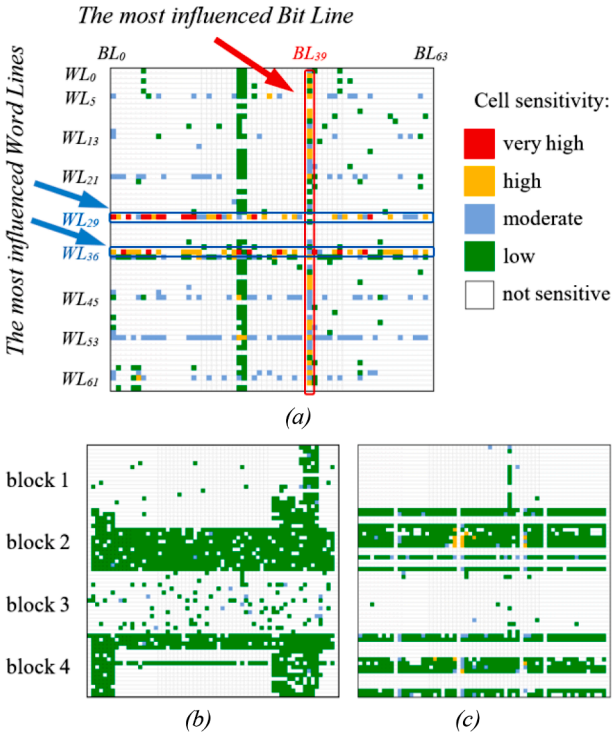


Fig. 22. The visualized overlaid matrix of: *(a)* – the chip #2; *(b)* – the chip #4; *(c)* – the chip #9.

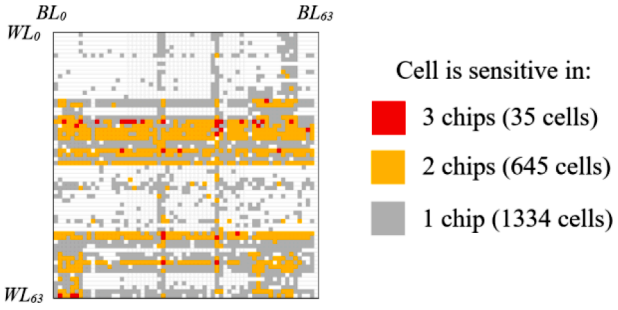


Fig. 23. The visualized overlaid matrix of cell sensitivity on all chips.

attacked chip and considering metal filler placements.

To estimate the influence of the metal fillers on the success of the laser influence we calculated the relation of the number of *observable laser influences* to the number of influenced cells for uncovered, partially covered as well as covered cells separately. Comparing the calculated relations we can conclude that the cells with "gaps" atop, i.e. those cells uncovered by metal fillers, are only slightly more sensitive to laser irradiation than partially covered or covered cells. Metal fillers seem to be an effective countermeasure as they are blocking the laser beam, but our experiments show that the MIM structures covered by metal fillers as well as the not covered ones were successfully influenced. Thus, the obvious solution – the use of metal fillers as a low-cost countermeasure – is rather questionable and requires additional experiments to understand which processes take place in RRAM cells during laser irradiation. In the next section we compare our results with other published works.

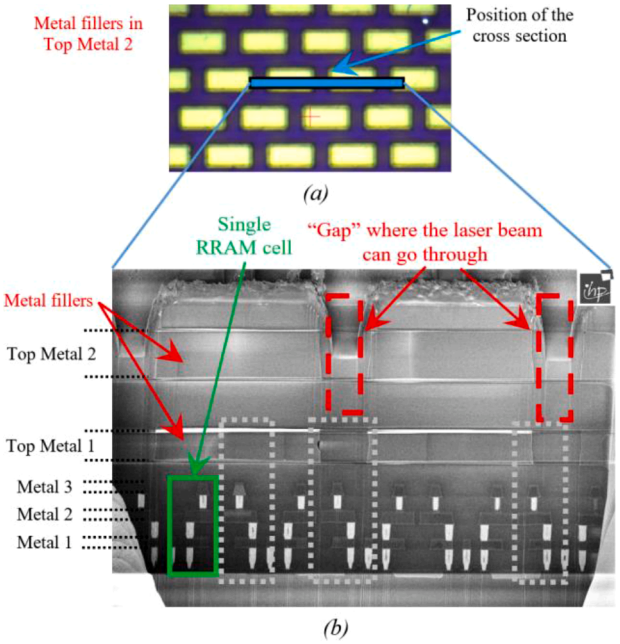


Fig. 24. Attacked RRAM chip: *(a)* – part of the chip surface, captured using 100× magnification objective; *(b)* – SEM cross section image (FIB cut) of the attacked RRAM chip.

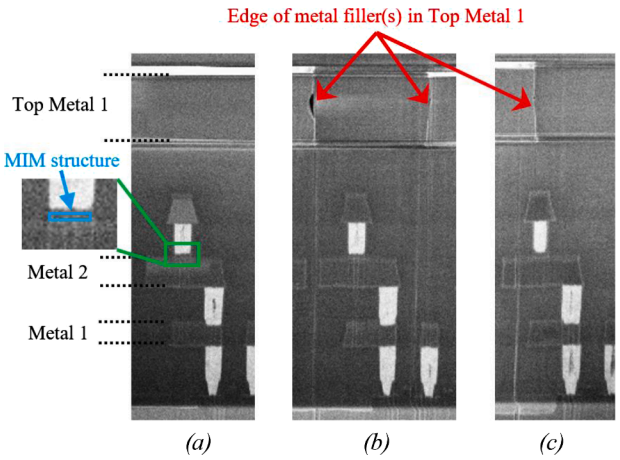


Fig. 25. Attacked RRAM cells, zoomed in: *(a)* – MIM structure covered by metal fillers; *(b)* – MIM structure not covered by metal fillers; *(c)* – MIM structure partially covered by metal fillers.

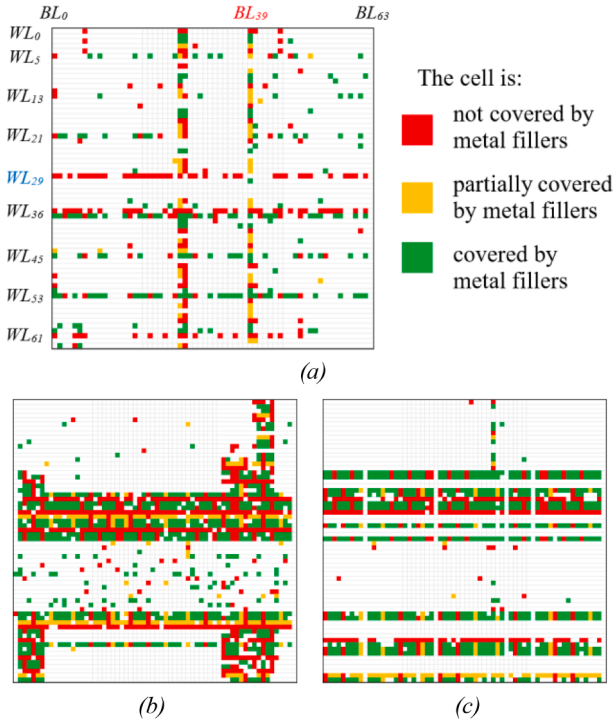


Fig. 26. Positions of influenced cells in the attacked chips considering metal fillers placement: *(a)* – chip #2; *(b)* – chip #4; *(c)* – chip #9.

7. Results comparison

Some works that investigated the sensitivity of RRAM cells to laser irradiation have already been published. In this comparison, we selected only publications that investigated HfO_2-based RRAM structures.

In [7] authors performed attacks on RRAM cells built in 1R architecture. The MIM structure of the attacked cell was built in a TiN/-Ti/HfO_2/TiN stack. To attack RRAM cells three laser sources were used: 355 nm, 533 nm and 1064 nm. The spot size was fixed to 50 μm. The authors reported that they successfully influenced RRAM cells that were programmed in HRS, i.e. transitions from HRS to LRS. All three laser sources used showed the same effect on the successfully attacked cells. So the authors concluded that the success of laser influence is independent of the laser wavelength. Moreover the authors showed that the observed transitions are caused by the temperature.

In [8] authors attacked the RRAM cells built in 1T-1R architecture. The MIM structure of the attacked cell was built in a TiN/Ti/HfO_2/TiN stack. To attack the RRAM cells a 1064 nm laser source was used. Attacks were performed with 50 ns pulse duration. The laser beam spot size was fixed to 5 μm. The authors observed transition of the attacked RRAM cells from HRS to LRS under laser exposure. Authors ascribe these transitions to temperature impact, i.e. heating that is caused by the laser.

In [9] the authors tested the RRAM cell based on a 1T-1R architecture in standalone and operational modes. The MIM structure of the attacked cell was built in a TiN/Hf/HfO_2/TiN stack. In [9] authors performed tests using laser source and heavy ion fluence. Here we focus on discussing their laser tests. Laser testing was carried out through the back-side with 1260 nm two-photon absorption (TPA) laser source. Laser tests were performed with 150 fs pulse duration and using a 100× magnification objective. The latter allowed to achieve the Gaussian spot

Table VI
Number of influenced cells in different modes for each chip considering metal fillers placement.

Chip Nr.	Number of analysed cells	Number of influenced cells	Number of *observable laser influences*	Analysed cells Not covered Number of the influenced cells	Number of *observable laser influences* for the influenced cells	Average number of influences per cell	Partially covered Number of the influenced cells	Number of *observable laser influences* for the influenced cells	Average number of influences per cell	Covered Number of the influenced cells	Number of *observable laser influences* for the influenced cells	Average number of influences per cell
#2	3143	434	786	200	406	2.03	51	84	1.65	183	296	1.62
#4	3597	1302	1324	518	527	1.02	183	186	1.02	601	611	1.02
#9	996	993	1076	306	340	1.11	106	112	1.06	581	624	1.07

size of 1.2 μm. Authors reported the inability to influence the standalone RRAM cell, i.e. no voltages to the cell are applied. Single RRAM cells were not susceptible to either laser irradiation or heavy ion fluence. However the authors were able to influence single RRAM cells that are supplied with operational voltages. In particular the authors observed the transitions from HRS to LRS of tested single RRAM cells. These transitions are ascribed to the influence on a NMOS transistor, i.e. charge collection in access transistor under laser irradiation.

In [10] authors attacked the RRAM cells based on a 1R architecture. The MIM structure of the attacked cell was built in a TiN/Ti/HfO_2/W stack. The authors performed attacks with three single-photon absorption (SPA) laser sources: 1064 nm, 1024 nm and 976 nm. Mainly the experiments were performed with 100 ns pulse duration and 25 μm spot size. However authors considered also a 3 μs pulse duration and Continuous Wave (CW) operation mode. The authors attacked RRAM cells with 12 μm and 3 μm laser spot sizes also. The authors did not observe any significant impact on the attacked RRAM cells during the laser irradiation in a pulsed mode. But they reported the damage of the RRAM cell when it was exposed to the 1024 nm laser source in CW mode. This damage was caused by the laser heating that burned the tested RRAM cell. Even though no faults were observed till the RRAM cell was damaged.

In [11] authors performed laser testing on a 1T-1R RRAM cell. The tested cell was based on a HfO_2 insulator layer. They used a TPA laser source with a wavelength of 1260 nm and a pulse duration of 150 fs. The authors observed transitions from HRS to LRS of the tested RRAM cells.

In [12] authors exposed a standalone RRAM chip to laser irradiation. The RRAM cells were based on HfO_X insulator layer and built in a 1T-1R architecture. To perform tests authors used an SPA laser source with a wavelength of 1064 nm. The experiments were carried out with 20 ps pulse duration and a spot size of 1.7 μm. Authors showed that the tested RRAM cells are robust to the single event effects since no transitions were observed.

TABLE VII gives a short summary articles discussed here. TABLE VII.

The results obtained in our work are different. On the contrary to the published works, in our experiments the RRAM cells programmed in LRS, i.e. the cells in logical state '1' and in 'Stuck-at 1' state, are likely to be influenced, see **Fig. 21**. Moreover, we are able to influence all logical states of the cells but with different success ratios. This can be due to:

- the use of a more powerful laser;
- inherent features of the RRAM cell implementation in IHP 250 nm technology, e.g. metal fillers;
- the number of laser shots performed on a single cell in our experiments, i.e. multiple shots between two consecutive READ operations.

Hence, our experiments show that it is possible to influence RRAM cells regardless of the programmed logical state.

8. Conclusion

In this work we investigated the sensitivity of the IHP RRAM chips to optical Fault Injection attacks. We demonstrated that precise localized injection of faults into RRAM chips using laser attacks can be successful. Laser irradiation can influence the state of the cell significantly, i.e. cells can change their logical state. States of the cells were successfully manipulated in all attacked IHP RRAM chips. Metal fillers seem to be an obvious and effective countermeasure as they are blocking the laser beam. But our experiments show that the success of optical FI attacks depends not significantly on the placement of metal fillers over the MIM structure of RRAM cell. Metal fillers may be a solution or part of a solution, but in order to determine this, the role/influence of the metal fillers on the effect of optical FI attacks needs further investigation.

Thus, the question how to protect RRAM cells against optical FI attacks is still open and countermeasures might well be independent of the placement of metal fillers.

Table VII
Overview Of Previously Published Works.

Ref.	Cell architecture	MIM structure	Laser source	Laser influence
[7]	1R	TiN/Ti/HfO_2/TiN	Wavelength: 355/533/1064 nm Spot size: 50 μm Pulse duration: 10 ns[a]	HRS to LRS
[8]	1T-1R	TiN/Ti/HfO_2/TiN[1]	Wavelength: 1064 nm Spot size: 5 μm Pulse duration: 50 ns	HRS to LRS
[9]	1T-1R	TiN/Hf/HfO_2/TiN	Wavelength: 1260 nm Spot size: 1.2 μm Pulse duration: 150 fs	HRS to LRS
[10]	1R	TiN/Ti/HfO_2/W	Wavelength: 1064/1024/976 nm Spot size: 25; 12; 3 μm Pulse dur.: 0.1; 3 μs	No transitions in RRAM cells
[11]	1T-1R	HfO_2-based	Wavelength: 1260[a] nm Spot size: 1.2[a] μm Pulse duration: 150[a] fs	HRS to LRS
[12]	1T-1R	HfO_x-based	Wavelength: 1064 nm Spot size: 1.7 μm Pulse duration: 20 ps	No transition in RRAM cells
This work	1T-1R	TiN/Ti/Al:HfO_2/TiN	Wavelength: 808 nm Spot size: 3×0.8; 6×1.5; 15×3.5; 60×14 μm^2 Pulse duration: 20 – 5•10^7 ns	HRS to LRS, LRS to HRS

[a] Not explicitly written.

Declaration of Competing Interest

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

ACKNOWLEDGMENT

This project has received funding from the European Union's Horizon 2020 research and innovation program under the Marie Skłodowska-Curie grant agreement No 722325.

Supplementary materials

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.micpro.2021.104376.

References

[1] L. Chua, Memristor-The Missing Circuit Element, IEEE Transactions on Circuit Theory 18 (5) (1971) 507–519. September.
[2] G. Dearnaley, A.M. Stoneham, D.V. Morgan, Electrical phenomena in amorphous oxide films, Rep. Prog. Phys. 33 (3) (1970) 1129.
[3] T.W. Hickmott, Low-Frequency Negative Resistance in Thin Anodic Oxide Films, J. Appl. Phys. 33 (9) (1962) 2669–2682. Sep.
[4] R. Waser, R. Dittmann, G. Staikov, K. Szot, Redox-Based Resistive Switching Memories – Nanoionic Mechanisms, Prospects, and Challenges, Adv. Mater. 21 (25-26) (2009) 2632–2663. Jul.
[5] S. Li, K. Seemakhup, G. Pekhimenko, A. Kolli, S. Khan, Janus, Optimizing Memory and Storage Support for Non-Volatile Memory Systems. Proceedings of ISCA 19, Phoenix, AZ, USA, 2019. June 22-26.
[6] D. Narayanan, O. Hodson, "Whole-system Persistence with Non-volatile Memories", 17th International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS 2012), March 2012.
[7] A. Krakovinsky, M. Bocquet, R. Wacquez, J. Coignus, D. Deleruyelle, C. Djaou, G. Reimbold, J.M. Portal, Impact of a laser pulse on HfO2-based RRAM cells reliability and integrity. Proceedings of the 2016 International Conference on Microelectronic Test Structures (ICMTS), Yokohama, Japan, 2016, pp. 152–156, 28-31 March.
[8] M.Bocquet Krakovinsky, R. Wacquez, J. Coignus, J.M. Portal, Thermal laser attack and high temperature heating on HfO2-based OxRAM cells. Proceedings of the 2017 IEEE 23rd International Symposium on On-Line Testing and Robust System Design (IOLTS), Thessaloniki, Greece, 2017, pp. 85–89, 3-5 July.
[9] W.G. Bennett, N.C. Hooten, R.D. Schrimpf, R.A. Reed, M.H. Mendenhall, M.L. Alles, J. Bi, E.X. Zhang, D. Linten, A. Fantini, Single- and Multiple-Event Induced Upsets in HfO2/Hf 1T1 R RRAM, IEEE Trans. Nucl. Sci. 61 (2014) 1717–1725.
[10] D. Arumí, S. Manich, Á. Gómez-Pau, R. Rodríguez-Montañés, V. Montilla, D. Hernández, M.B. González, F. Campabadal, Impact of Laser Attacks on the Switching Behavior of RRAM Devices, Electronics 200 (2020) 9.
[11] J. Bi, Z. Han, Mitigation of soft errors in resistive switching random-access-memories. Proceedings of the 2014 IEEE International Conference on Electron Devices and Solid-State Circuits, Chengdu, China, 2014, pp. 1–2, 18-20, June.
[12] X. Kai, Z. Feng, L. Jin, J. Lanlong, F. Cong, L. Jing, L. Ming, B. Jinshun, Pulsed-laser testing for single event effects in a stand-alone resistive random access memory. Proceedings of the 2017 IEEE 24th International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA), Chengdu, China, 2017, pp. 1–4, 4-7 July.
[13] D. Walczyk, C. Walczyk, T. Schroeder, T. Bertaud, M. Sowiska, M. Lukosius, M. Fraschke, B. Tillack, C. Wenger, Resistive switching characteristics of cmos embedded HfO2-based 1T1 R cells, Microelectronic Engineering 88 (7) (2011) 1133–1135.
[14] S.R. Ovshinsky, Reversible electrical switching phenomena in disordered structures, Physical review letters 21 (20) (1968) 1450–1453. Nov.
[15] N.R. Rao, G.V. Subba Rao, Transition Metal Oxides. Crystal Chemistry, Phase Transition and Related Aspects, U. S. National Bureau of Standarts, 1974, p. 138. Issued June.
[16] IUPAC, Compendium of Chemical Terminology, 2nd ed. (the "Gold Book") (1997). Online corrected version: (2014) "transition element." 10.1351/goldbook.T06456.
[17] M. Orchin, R. S. Macomber, A. Pinhas, and R. M. Wilson, "The Vocabulary and Concepts of Organic Chemistry", 2nd ed., 2005, 24 p.
[18] D. Walczyk, T. Bertaud, M. Sowinska, M. Lukosius, M.A. Schubert, M. Fraschke, A. Fox, D. Wolansky, A. Scheit, M. Fraschke, G. Schoof, Ch. Wolf, R. Kraemer, B. Tillack, R. Korolevych, V. Stikanov, Ch. Wenger, T. Schroeder, Ch. Walczyk, Resistive switching behavior in TiN/HfO2/Ti/TiN devices. 2012 International Semiconductor Conference Dresden-Grenoble (ISCDG), Grenoble, 2012, pp. 143–146.
[19] Panasonic ReRAM Product. URL: https://industrial.panasonic.com/ww/products/semiconductors/microcomputers/mn101l (last accessed: 22 Dec 2020).
[20] Fujitsu ReRAM Product. URL: https://www.fujitsu.com/global/products/devices/semiconductor/memory/reram/spi-4m-mb85as4mt.html (last accessed: 22 Dec 2020).
[21] Adesto Technologies RRAM Product. URL: https://www.rram-info.com/adesto-technologies (last accessed: 22 Dec 2020).
[22] IHP Embedded RRAM. URL: https://www.ihp-microelectronics.com/en/research/materials-for-micro-and-nanoelectronics/projects/embedded-rram.html (last accessed: 22 Dec 2020).
[23] IHP BiCMOS technology. URL: https://www.ihp-microelectronics.com/en/services/mpw-prototyping/sigec-bicmos-technologies.html (last accessed: 22 Dec 2020).
[24] A. Padovani, L. Larcher, P. Padovani, C. Cagli, B. De Salvo, Understanding the Role of the Ti Metal Electrode on the Forming of HfO2-Based RRAMs. 2012 4th IEEE International Memory Workshop, Milan, 2012, pp. 1–4, https://doi.org/10.1109/IMW.2012.6213667. May.
[25] C. Walczyk, C. Wenger, D. Walczyk, M. Lukosius, I. Costina, M. Fraschke, J. Dabrowski, A. Fox, D. Wolansky, S. Thiess, E. Miranda, B. Tillack, T. Schroeder,

On the role of Ti adlayers for resistive switching in HfO2-based metal-insulator-metal structures: Top versus bottom electrode integration, J. Vac. Sci. Technol. B. 29 (2011) 01AD02. Jan/Feb.
[26] S. Dirkmann, J. Kaiser, C. Wenger, T. Mussenbrock, Filament Growth and Resistive Switching in Hafnium Oxide Memristive Devices, ACS Applied Materials & Interfaces 10 (17) (2018) 14857–14868, https://doi.org/10.1021/acsami.7b19836.
[27] Perez, et al., Characterisation of the interface-driven 1st Reset operation in HfO2-based 1T1 R RRAM devices, Solid State Electronics 159 (2019) 51–56.
[28] Active Technologies RIFLE. Non Volatile Memory Testers. URL: https://www.activetechnologies.it/products/non-volatile-memory-testers/.
[29] A. Grossi, C. Zambelli, P. Olivo, E. Miranda, Valeriy Stikanov, T. Schroeder, C. Walczyk, C. Wenger, Relationship among Current Fluctuations during Forming, Cell-To-Cell Variability and Reliability in RRAM Arrays. 2015 IEEE International Memory Workshop (IMW), Monterey, CA, 2015, pp. 1–4.
[30] C. Walczyk, D. Walczyk, T. Schroeder, T. Bertaud, M. Sowinska, M. Lukosius, M. Fraschke, D. Wolansky, B. Tillack, E. Miranda, C. Wenger, Impact of Temperature on the Resistive Switching Behavior of Embedded HfO2-Based RRAM Devices, IEEE Transactions on Electron Devices 58 (9) (2011) 3124–3131. Sept.
[31] Riscure. Diode Laser Station Datasheet, 2011. URL: https://www.riscure.com/security-tools/inspector-hardware/.
[32] V.Pouget Lewis, F. Beaudoin, P. Perdu, H. Lapuyade, P. Fouillat, A. Touboul, Backside Laser Testing of ICs for SET Sensitivity Evaluation, IEEE Transactions On Nuclear Science 48 (6) (2001) 2193–2201. Dec.
[33] Riscure. VC Glitcher Datasheet, 2011. URL: https://www.riscure.com/uploads/2017/07/datasheet_vcglitcher.pdf (last accessed: 22 Dec 2020).
[34] Riscure. Security tool. Inspector Fault Injection. URL: https://www.riscure.com/security-tools/inspector-fi/ (last accessed: 22 Dec 2020).
[35] Märzhäuser Wetzlar GmbH & Co. Tango desktop. URL: https://www.marzhauser.com/de/pim/produktdetail-popup.html?view=details&pimid=a182&nocache=1&m=null&p=null (last accessed: 06 Nov 2019).
[36] D. Petryk, Z. Dyka, E. Perez, M.K. Mahadevaiaha, I. Kabin, Ch. Wenger, P. Langendörfer, Evaluation of the Sensitivity of RRAM Cells to Optical Fault Injection Attacks. 2020 23rd Euromicro Conference on Digital System Design (DSD), Kranj, Slovenia, 2020, pp. 238–245.
[37] D. Petryk, Z. Dyka, J. Katzer, P. Langendörfer, Metal Fillers as Potential Low Cost Countermeasure against Optical Fault Injection Attacks. 2020 IEEE East-West Design & Test Symposium (EWDTS), Varna, Bulgaria, 2020, pp. 1–6.
[38] M.K.Mahadevaiah, Perez, E.P.-B. Quesada, C. Wenger, Variability and Energy Consumption Tradeoffs in Multilevel Programming of RRAM Arrays, IEEE Transactions on Electron Devices 68 (6) (2021) 2693–2698. June.

Dmytro Petryk received his Diploma degree in Radio Engineering from Taras Shevchenko National University of Kiev, Ukraine, in 2017. Since 2018, he is with the IHP-Leibniz Institut für innovative Mikroelektronik, Frankfurt (Oder), Germany and a student in Technical University of Cottbus-Senftenberg, Germany. His research interests include fault injection attacks and countermeasures against them.

Zoya Dyka received her Diploma degree in Radiophysics and Electronics from Taras Shevchenko University Kiev, Ukraine in 1996 and the Ph.D. degree from Technical University of Cottbus-Senftenberg, Germany in 2012. Since 2000 she is with the IHP in Frankfurt (Oder). Since 2013, she has been leading a young researchers group in the field of tamper resistant crypto ICs. Since 2018, she is leading a research group in the field of resilient CPSoS. She has authored more than 30 peer reviewed technical articles and filed five patents in the security area of which four are granted. Her research interests include design of efficient hardware accelerators for cryptographic operations, SCA countermeasures, anti-tampering means and resilience.

Eduardo Perez received the M.Sc. and Ph.D. degrees in Information and Communications Technologies from University of Valladolid (Spain) in 2010 and 2014, respectively. He has been with the IHP-Leibniz-Institut für innovative Mikroelektronik since 2015, where he has worked in the field of resistive switching (RRAM) devices for implementing emergent non-volatile memories and hardware-based artificial neural networks.

Ievgen Kabin received the Diploma degree in Electronic Systems from the National Technical University of Ukraine "Kyiv Polytechnic Institute'', Kiev, Ukraine, in 2009. From 2009 to 2010, he was a Leading Engineer with the state-owned enterprise, Scientific Production Center of Energy-efficient Designs and Technologies, ("Tehnoluch"). From 2010 to 2015, he was a Junior Researcher with the E.O. Paton Electric Welding Institute, National Academy of Sciences of Ukraine. Since 2015, he is with IHP-Leibniz Institut für innovative Mikroelektronik, Frankfurt (Oder), Germany. There he is a member of the research group Sensor Networks and Middleware Platforms Groupand published more than 15 articles. His research interests include side-channel analysis attacks and investigations in the field of Elliptic Curve Cryptography.

Jens Katzer was born in Erfurt, Germany, in 1958. He received the degree of a Diploma Physicist from the Humboldt University Berlin in 1984. Between 1984 and 1991 he worked as an engineer of development for material researches, surface analysis, and failure analysis of semiconductor devices, especially with the method of Auger Electron Spectroscopy (AES), in the Halbleiterwerk Frankfurt (Oder). Between 1992 and 2001 he was engaged as a project manager in the municipal administration of Frankfurt (Oder). Between 2001 and 2008 he worked as a project engineer in the company GreenWay Systems GmbH in Frankfurt (Oder), a company for development and manufacture of systems of traffic telematics, like mobile traffic management systems and a priority switching of traffic lights for emergency and rescue vehicles. Now his tasks in the Offline-Characterization group in Technology Department of IHP Frankfurt (Oder) are investigations by Focused Ion Beam (FIB) and other methods of material research.

Jan Schäffner received his B.Eng. in mechanical engineering and mechatronic from bbw Hochschule - University of Applied Science Berlin in 2012. Since 2003 he has been working as a science-based technician, later engineer in the systems department at IHP. Since 2014 he has been responsible for packaging, assembly and system integration of microelectronic components, especially bare die assembly and integration. His primary area of interest include advanced packaging and systems integration technologies.

Prof. Dr. Peter Langendörfer holds a diploma and a doctorate degree in computer science. Since 2000 he is with the IHP in Frankfurt (Oder). There, he is leading the wireless systems department. From 2012 till 2020 he was leading the chair for security in pervasive systems at the Technical University of Cottbus-Senftenberg. Since 2020 he owns the chair wireless systems at the Technical University of Cottbus-Senftenberg. He has published more than 145 refereed technical articles, filed 17 patents of which 10 have been granted already. He worked as guest editor for many renowned journals e.g. Wireless Communications and Mobile Computing (Wiley) and ACM Transactions on Internet Technology. Peter is highly interested in security for resource constraint devices, low power protocols and resilience.