Dual Detection of Heating and Photocurrent attacks (DDHP) Sensor using Hybrid CMOS/STT-MRAM

M. Kharbouche-Harrari, R. Wacquez, G. Di Pendina, J.-M. Dutertre, J. Postel-Pellerin, D. Aboulkassimi, J.-M. Portal

Dual Detection of Heating and Photocurrent attacks (DDHP) Sensor using Hybrid CMOS/STT-MRAM

M. Kharbouche-Harrari*,[1,2,3], R. Wacquez[1], G. Di Pendina[3], J.–M. Dutertre[4], J. Postel-Pellerin[2], D. Aboulkassimi[1], and J.-M. Portal[2]

1. CEA Tech, Centre CMP, Equipe Commune CEA Tech - Mines Saint-Etienne, F-13541 Gardanne France
2. Aix-Marseille Univ., CNRS, IM2NP, 13397 Marseille Cedex 20, France
3. Univ. Grenoble Alpes, CNRS, CEA, IRIG-SPINTEC, 38000 Grenoble, France
4. Mines Saint-Etienne, CEA-Tech, Centre CMP, F - 13541 Gardanne France
*corresponding author: Mounia.Kharbouche@cea.fr

Abstract — **Integrated Circuits (ICs) have to be protected against threatening environmental radiations and malicious perturbations. A large panel of countermeasures has been developed to answer the needs of this challenging field. The Bulk Built-In Current Sensor (BBICS) is a highly reliable solution for the detection of these abnormal transient radiations that could induce a transient current in the Front-End of Line (FEoL). This paper proposes an innovative sensor based on the BBICS associated to the power-efficient emerging non-volatile memory Spin Transfer Torque Magnetic Random Access Memory (STT-MRAM). The goal of this security solution is to detect both possible photoelectrical laser injections and thermal perturbations. Thus, the proposed architecture designated by Dual Detection of Heating and Photocurrent attacks (DDHP) highlights a dual detection efficiency, on the CMOS circuitry and on the Back-End of Line (BEoL) STT-MRAM technology.**

Keywords — DDHP, BBICS, STT-MRAM, laser attack, sensor.

I. INTRODUCTION

With the microelectronics downscaling, Integrated Circuits (ICs) have to be hardened in order to prevent natural or human alteration of the system operation [1]. While for the natural aggressions, one can cite aging and environmental radiations [2], human intentional attacks on another note, are mainly generated by physical aggressions of the IC. Thus, during the computation of a cryptographic algorithm, faults are injected in specific locations of the IC and at the right time, making possible the retrieval of the secret key [3]. These physical attacks evolved in the last years from a global circuit alteration using temperature or voltage glitch to local aggressions. Among the means used to generate faults into ICs in hardware security characterization, laser injection offers a high spatial (in the order of magnitude of 1µm) and temporal accuracy. The radiation community first introduced this technique to emulate Single Event Effects (SEE) inducing transient faults in ICs [4], [5]. Front-End of line (FEoL) laser injection induces transient faults in ICs via photocurrent generation [6].

In order to prevent these attacks and to secure the architectures, several sensors [1], [7], [8] have been proposed, mainly to detect errors that are induced in the CMOS bulk. The use of a sensor in sensitive ICs is required in order to detect a fault injection tentative, even before it leads to exploitable faults. In the detection structures landscape, the Bulk Built-In Current Sensor (BBICS) is a good candidate, for advanced technology nodes, to monitor transient currents induced in the bulk of the IC by a laser illumination for instance [9], [10].

As identified by the International Technology Roadmap for Semiconductors (ITRS), STT-MRAM technology is one of the most promising technologies for a wide range of applications in the emerging non-volatile memory landscape [11] mostly for the Internet of Things (IoT). This type of memory is foreseen to replace some SRAM memories used as embedded working memory in order to become a universal memory. Thus, their hardening and robustness is essential. Recently, it has been demonstrated that front-side laser injection may also generate faults on the Back-End of Line (BEoL) of emerging non-volatile memories such as Resistive Random Access Memory (RRAM) [12] or Spin Transfer Torque Magnetic Random Access Memory (STT-MRAM) [13]. Thus, it is now mandatory to also detect laser attacks targeting the STT-MRAM.

In this aim, this paper proposes an innovative sensor in order to secure both the FEoL and the BEoL of the ICs. This new dual sensor solution, named Dual Detection of Heating and Photocurrent attacks (DDHP), detects the threats targeting the CMOS technology via the generation of a photoelectrical current and the threats targeting the emerging non-volatile memories embedded in the BEoL via a heating perturbation. This sensor solution is simulated on a 28nm FD-SOI technology node platform coupled to a perpendicular-to-plane 40nm STT-MRAM technology. The proposed sensor is efficient in analogue manner for a bulk CMOS PDK. Even though the FD-SOI technology is less sensitive than the bulk CMOS, both involve a similar mechanism [14].

This paper is organized as follows: Section II provides the background of this study. Section III describes the proposed dual architecture to sense photoelectrical and thermal perturbations. Section IV evaluates the proposed architecture. Finally, Section V gives concluding remarks.

II. BACKGROUND

A. Laser injection on integrated circuits

Light Amplification by Stimulated Emission of Radiation (LASER) is a coherent and unidirectional electromagnetic radiation. Laser injection main features have made it a tool of choice in reliability studies and security of electronic devices since it outlines an accurate spatial and temporal resolution [15]. Laser illumination of integrated circuits can generate two fault models on the circuit operation: photoelectrical faults or thermal faults.

1) Photoelectrical effect

The photoelectrical effect is defined by the effect of the light on the matter. Thus, in the volume of interaction, electron-hole pairs are generated. Some of the electrical charges inherently recombine without particular effect on the IC,while the others are collected in presence of an electrical field generated in reverse biased PN junctions, generating a transient current that may engender faults in the IC. This photocurrent may achieve an amplitude of a few mA and lasts a few hundreds of picoseconds [14].

In the CMOS circuits, the most sensitive regions are the PN junction of the "OFF" transistors. In the case of a laser injection, the energy needed by a particle to create a transient current is proportional to the wavelength of the laser beam. This photocurrent pulse vanishes as the charges are drained. This technology presents ? three sensitive regions where a transient current may be induced in the volume, as shown in Figure 1.a:

- For an NMOS transistor, the PN junction defined by the P type substrate and the doped N+ region (zone (1)).
- For a PMOS transistor the PN junctions defined by:
  - The P type substrate and the N type well (zone (2)).
  - The doped P+ region and the N type well (zone (3)).

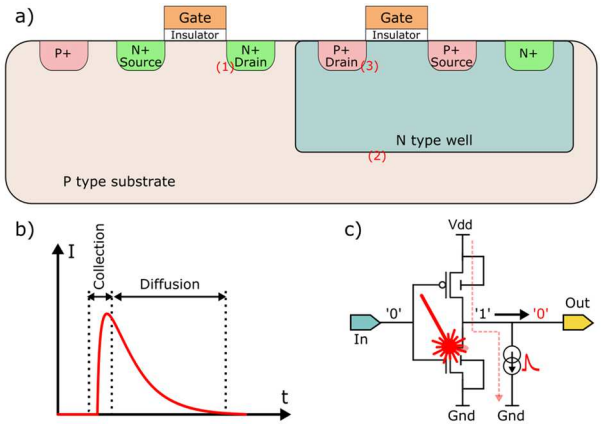


Figure 1: a) Cross sectional view of the CMOS technology. b) Induced transient current after a laser illumination. c) Current injection on the drain of an NMOS transistor switching the inverter's output from '1' to the faulty value '0'.

The charges generating the photocurrent are carried through the structure and decomposed into collection (charges collected in a few picoseconds inducing a peak current) and diffusion (the current decreases until all the charges are collected) [14], as illustrated in Figure 1.b. The charge carriers (electrons and holes) collected at one of these three sensitive regions create a transient current in the transistor. Figure 1.c highlights a laser illumination targeting the PN junction of the NMOS transistor (zone (1) in Figure 1.a), thus the inverter output switches from '1' to the faulty value '0'.

2) Thermal effect

Other than the photocurrent induced by a laser perturbation, a new attack methodology that threats the integrated circuits and mainly the memory chips has been introduced by Skorobogatov in 2009 [16]. It has been demonstrated that the local heating of the chip may induce memory errors in Flash memories and thus cause the leakage of confidential data. This work paved the way for the use of the laser irradiation as an ideal heat source that affects the non-volatile memories circuitry with a high spatial accuracy. After the exposure of the sensitivity of microelectronics chips to the heating effect of a laser source, several works determined the weaknesses and strengths of the non-volatile memories and their ability to be embedded in the ICs.

Recent works evaluated the thermal effect impact on emerging non-volatile memory induced by a laser irradiation, on the OxRAM technology [12] and on the STT-MRAM memory [13]. This thermal effect is mostly induced by front-side laser injections. This heat is transferred from the sample surface to the lower metal layers [17].

B. *Bulk Built-In Current Sensor (BBICS)*

Multiple sensors are being developed in order to prevent and detect transient faults in the ICs, as resumed in [1]. One of the most attracting architectures in this landscape for its high potential in detecting invasions targeting the FEoL is the Bulk Built-In Current Sensor (BBICS [8]). Each current injection in the P type substrate "Pwell" or in the N type well "Nwell" raises a flag notifying the user of this attack (or attempt). "Pwell" and "Nwell" are concurrently monitored by respectively the pull-up and pull-down of the CMOS networks [8], as conceptually shown in Figure 2.a. Thus, this structure is an external sensor that monitors the transient current that is induced by a laser source at the FEoL of the IC. Since it has been proposed in [9], [10], the BBICS detector is one of the most investigated as in [18]–[20] so as to outperform its strengths.

To initialise the circuit, a reset signal ('rst') is generated in the cross-coupled inverters outputs ('out' and '$\overline{\text{out}}$'). For the steady state of the BBICS structure, the output 'out' is set to '0' through transistor M_{n0} (resp. the output '$\overline{\text{out}}$' is set to '1' via transistor M_{p1}). When a perturbation generates a transient

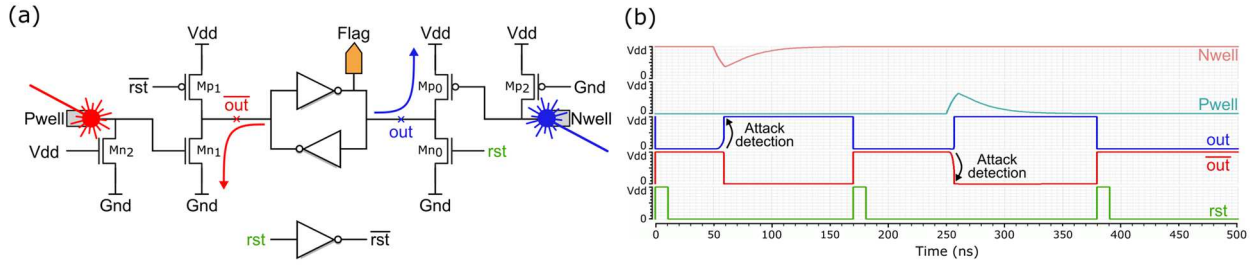


Figure 2: Bulk Built-In Current Sensor (BBICS) operating structure. a) Schematic of the structure highlighting the detection of an attack for induced currents into the N type well and the P type substrate. b) Simulation of the structure and verification of its operation. Detection of an abnormal current induced in the "Nwell" (1st detection) and in the P substrate "Pwell" (2nd detection).

current in the structure, the BBICS raises a flag by switching 'out' and '$\overline{out}$' to '1' and '0', respectively.

For an attack disturbing the "Pwell" of the device, the photocurrent is drained to the ground of transistor M_{n2}. When the V_{ds} voltage of transistor M_{n2} gets sufficient, the command voltage V_{gs} of M_{n1} increases up to the activation of the transistor. Therefore, the awakening of transistor M_{n1} draws '$\overline{out}$' to the ground. The feedback loop of the inverters pulls 'out' to "Vdd", rising the flag of the attack detection. In the case of the establishment of a transient current in the N type well "Nwell", in an analogue manner, transistors M_{p0} and M_{p2} draw 'out' to '1' and thus rises the dedicated flag, as illustrated in Figure 2.a.

The core latch sensitivity is designed to detect small variations at its input voltages. This accuracy is defined by the scaling of the transistors M_{p0} and M_{n1}. The higher the W/L ratio of these transistors, the more sensitive is the latch. It has to be noted that after the flag has been raised after a laser irradiation induced by the transient bulk current, the latch stays locked in detection-mode (flag up). So, it is necessary to reset the architecture after each detection, as shown in Figure 2.b, through the reset signal 'rst'.

C. *The Perpendicular-to-plane STT-MRAM technology*

The perpendicular Spin Transfer Torque Magnetic Random Access Memory (STT-MRAM) technology showcases low voltage operation enabling its hybridisation with the CMOS process, low power consumption and high scalability and density [21]. The STT-MRAM nano-pillar is based on a Magnetic Tunnel Junction (MTJ) [22]. The MTJ hetero-structure consists of two ferromagnetic layers separated by an insulating tunnel barrier [23], as illustrated in Figure 3.a. The ferromagnetic magnetisation is preferred along an easy axis perpendicular-to-plane.

This memory technology has two steady states: Parallel and Anti-Parallel. While the storage layer of the MTJ has the same (resp. the opposite) magnetisation as the reference layer, then the junction is in a Parallel P (resp. Anti-Parallel AP) state with a resistivity denoted R_P (resp. R_{AP}). The P state (resp. AP state) corresponds to a low (resp. high) resistivity associated to a logical '0' (resp. '1'). Figure 3.b illustrates the energy E_k requested for a junction to remain in an intermediate magnetisation in-between P and AP. Intrinsically the material will always choose a magnetization needing a minimal energy. The switching is thus only possible from a P to AP magnetisation and inversely.

A spin-polarised current that is carried through this nanostructure induces the switching operation in the MTJ. Depending on the current direction, one of the two MTJs states is written as shown by Figure 3.c.

Figure 3.d outlines the physical parameters and values used in order to simulate the STT-MRAM bit-cell, using a compact model.

D. *STT-MRAM robustness*

This memory bit-cell has been chosen in order to detect thermal (mostly front-side) perturbations since as demonstrated in [13], STT-MTJ integrity can be altered by front-side IR-laser beam injections, with a 1064nm wavelength. Given an adequate energy (547nJ) provided by laser illumination, an MTJ in an AP magnetisation reverses to a P orientation. The "one-way" fault model illustrated for this memory technology is a bit-reset model, switching the structure from the high resistive state '1' to the low resistive state '0'. For a junction in a P initial position, its resistivity and magnetic orientation are not altered by laser irradiation.

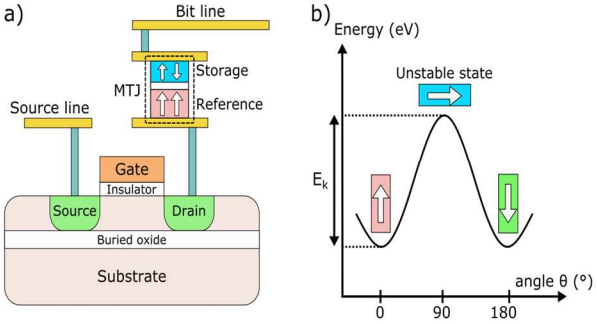
In this perspective, the use of an STT-MRAM matrix initialized into the AP polarisation, to detect any intrusion at the chip's surface is a good candidate and almost mandatory for the development of a front-side countermeasure.

III. PROPOSED DDHP DUAL STRUCTURE

This work purpose is to detect photoelectrical (mainly on the backside) and thermal (mostly on the front-side) perturbations by combining the backside sensing solution BBICS with the use of the perpendicular-to-plane STT-MRAM technology. This innovative architecture provides a high security contribution enabling the detection at the same time of FEoL and BEoL irradiations. The proposed hardware solution is designated by Dual Detection of Heating and Photocurrent attacks (DDHP). This sensor solution is simulated, for this case study, on a 28nm FD-SOI technology node coupled to a perpendicular-to-plane 40nm STT-MRAM technology. The efficiency of the proposed sensor is equivalent for a bulk CMOS PDK. As stated in [14], even though the FD-SOI technology is less sensitive than the bulk CMOS, both involve a similar mechanism.

A. *Sensing operation*

The proposed architecture is based on the BBICS sensing operation for fault injections on the "Pwell" or on the "Nwell" coupled to a structure that grants the detection of the resistivity alteration of the MTJ_{sense} junction, as shown in Figure 4.



d)

Symbol	MTJ Parameter description	Model value
P-STT-MRAM	Magnetic anisotropy	perpendicular
TMR	Tunnel Magneto-Resistance (%)	150
d_{MTJ}	MTJ diameter (nm)	40
RA	Resistance Area product (Ω.µm²)	1.25
α	Gilbert Damping	0.008
W	Minimum transistor width (nm)	80
L	Minimum transistor length (nm)	30
Vdd	Supply voltage (V)	1

Figure 3: The perpendicular STT-MRAM technology overview. a) Illustration of the STT-MRAM and the Magnetic Tunnel Junction (MTJ) based on a FD-SOI technology. b) Depiction of the steady states (P and AP) of this technology. c) Resistivity evolution as a function of the induced current in the structure. d) Physical properties and simulation setup of the STT-MRAM bit-cell.

The reading/sensing operation is realised by comparing the MTJ_{sense} resistivity to a reference MTJ_{ref}. This reference value is chosen as the median value of R_{AP} and R_P.

Since the initial feedback loop state is for 'out' at the '0' logical level and '$\overline{out}$' at the high logical level (in the standby position), in order to detect a modification of the MTJ_{sense} resistance, this junction is connected to '$\overline{out}$' while the reference is connected to 'out'. Actually, while the circuit is in standby mode, the MTJ_{sense} resistivity is restored into the latch and thus the node '$\overline{out}$' is set to '1' (MTJ_{sense} still in the AP magnetization) and 'out' remains in the low position.

The thermal stress detection operation is performed by the two transistors M_{nRd1} and M_{nRd2} controlled by the reading signal 'Rd', as shown in Figure 4. Then, depending on the resistivity of the MTJ_{sense} junction, '1' denoting the absence of any perturbation on the STT-MARM technology and '0' announcing an attack, the system operation differs. If the stored value into the MTJ_{sense} junction corresponds to a logic '1' (high resistivity), this value is compared to the reference (mid-state resistivity), both junctions discharge through the transistors M_{nRd1} and M_{nRd2}. The lower resistance branch discharges faster than the higher resistance branch. Hence, logic '1' is then restored into the node '$\overline{out}$' (charged to "Vdd") and '0' into the node 'out'. The system stays in a "No detection" mode.

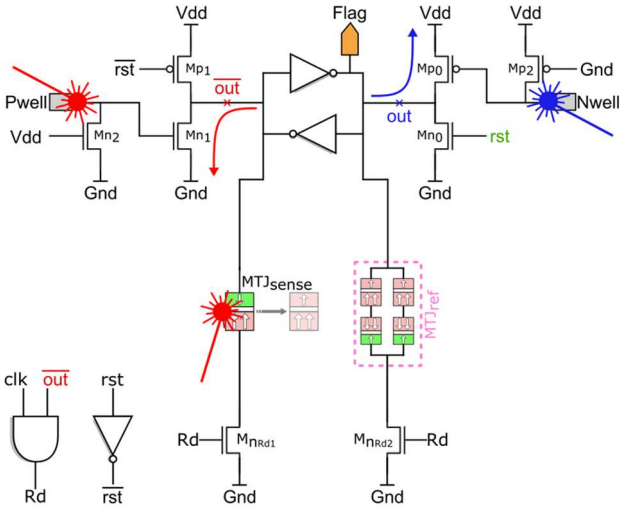


Figure 4: proposed architecture of the detector in the sensing mode.

In a complementary manner, if the MTJ_{sense} has been switched from the AP polarisation to the P magnetisation, then the branch that discharges faster due to its lower resistivity is the one connected to '$\overline{out}$'. Due to the feedback, '1' is written into the 'out' node, rising the flag notifying the attack.

As illustrated in Figure 4, the overhead needed to sense the information stored in the sensing junction is limited to the addition of 2 transistors and an AND logical gate. The AND gate aims at realising a clocked reading operation with a given frequency. The reading frequency of this operation depends on the targeted application. For instance, for a high security demand, the frequency would need to be elevated whereas for a standard security level, the circuit's clock could be sufficient. This reading operation is only done in case no detection has already been induced into the DDHP detector. If an attack is monitored on the FEoL, no reading operation is performed before the complete reset of the architecture.

B. Programming operation on the MTJs

Ensuing an attack, just as the BBICS has to be reset, the MTJ_{sense} has to be written back to the AP state. Moreover, this programming scheme also allows writing the reference junctions back to the AP state and the P one.

Indeed, to ensure in the reference that two junctions are written into the P state and the two others into the AP magnetisation, each two serial junctions are inter-connected by their reference layers, as illustrated in Figure 4 and in Figure 5. The current is for the first serial MTJ injected through the storage layer (junction written to the AP state) while it is injected through the reference layer for the second MTJ in serial (junction written into the P state). This disposition in the reference junctions grants to always compare the sensing junction to a mid-resistivity reference.

Figure 5 illustrates the area overhead needed to write the MTJs junctions. As stated, this overhead is limited to the addition of 3 transistors (M_{nWrE0}, M_{nWrE1} and M_{pWrE1}) and an inverter logical gate. The current flows from "Vdd" through M_{pWrE1}transistor writing the AP magnetization into the MTJ_{sense} junction, this current is then conduced by the transistor M_{nWrE0} and is divided into two components that write the reference (2 junctions into the AP orientation and 2 junctions into the P magnetisation, guaranteed by design).

To this MTJ writing circuitry, an inverter was added, controlled by the writing signal 'WrE' in order for its output to activate the PMOS transistor while the NMOS transistors are enabled by the signal 'WrE'.

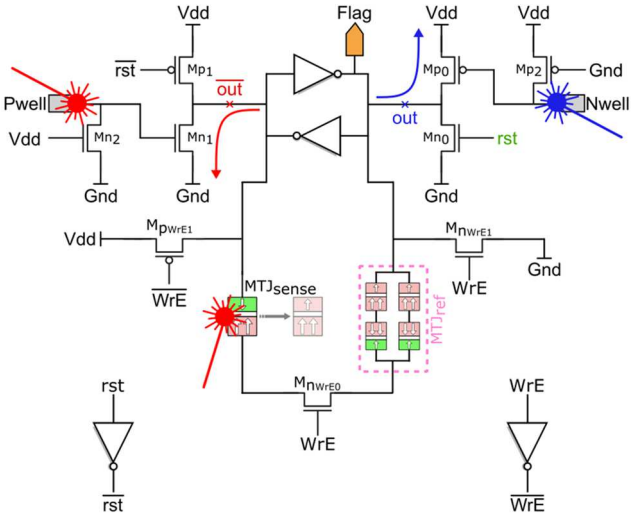


Figure 5: Reprogramming scheme of the MTJs.

C. Attack on the reference

This architecture is efficient even if an experimented attacker targets the reference junctions and not the sensing junction. This perturbation path (disrupted reference) has to be taken into account while realising the layout of the circuit. In fact, one of the easiest solutions would be to bring the sensing junction and the reference junctions that are in the AP magnetisation as close as possible. Therefore, whenever the attacker aims the reference, it would be impossible to switch the reference without switching the sensing junction. Therefore, the structure would still detect any attack in this case. Moreover, the accuracy of this detection may be outperformed by unbalancing the size of the sensing transistors M_{nRd1} and M_{nRd2}. For a M_{nRd1} W/L ratio higher

than M_{nRd2} W/L ratio, the sensing ability of this architecture is highly enhanced.

D. General operation

The general architecture of the DDHP sensor is composed of the sensing/writing circuits for MTJs, coupled with the BBICS structure as illustrated in Figure 6. Thus, this architecture can sense several attack models, backside (for photoelectrical invasions mainly) through the BBICS and on front-side through the sensing operation of the MTJs (invasions mainly induced by a thermal effect on the STT-MRAMs).

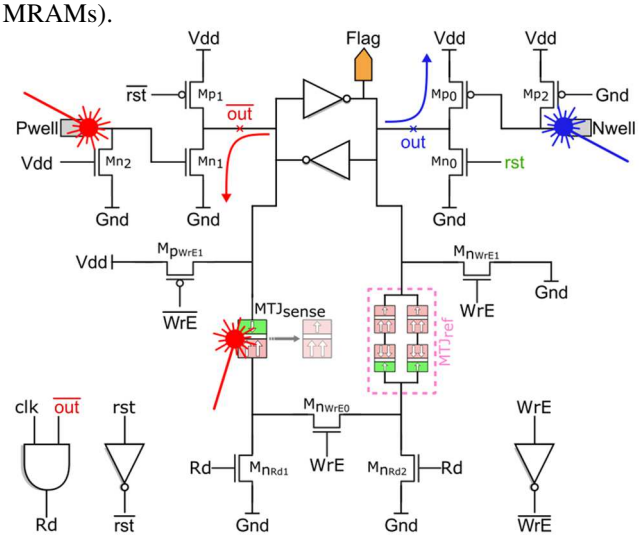


Figure 6: Complete structure of the proposed DDHP sensor.

IV. Evaluation of the DDHP operation

~~3)~~1) Electical simulation of the proposed solution

As demonstrated in Figure 7, the dual photoelectrical and thermal detection is functional for different fault injection techniques. As depicted, whereas the 1st and 3rd detections were induced by the BBICS that detected an abnormal bulk current in the "Nwell" and in the "Pwell" respectively, the 2nd detection was induced by the dynamic reading of the MTJ_{sense}. The MTJ has been switched from an AP state to a P one by a laser illumination for instance.

After each detection, the structure has to be reset through the 'rst' signal and the junction has to be written to grant the AP initialization state in the MTJ_{sense} by applying the 'WrE' signal with a period t_{write} on the sensing and reference MTJs. After the reset of the circuit, the MTJ_{sense} is set to the logical value '1' (high resistivity - R_{AP}). No modification is observed on the nodes 'out' and '$\overline{out}$' (verifications made at $t = 330ns$ and $t = 490ns$). Thus, this structure do not introduce false positive faults (flag raised whereas no attack was meant). For the illustrated simulation, the writing pulse duration of the MTJs is equal to 15ns, to program the sensing junction and the references. This duration can be reduced down to 1.1ns to realise only the MTJ_{sense} writing to the AP state. The sensing signal corresponds to a 1V pulse with a duration of 80ps.

~~1)~~2) Monte Carlo simulation of the proposed architecture

To evaluate its robustness, the DDHP architecture was simulated using the Monte Carlo (MC) methodology by implementing a 1,000 rounds simulation to verify the structure operation as stated in Figure 8. This MC simulation was done for a given Tunnel Magneto-Resistance (TMR corresponding to $(R_{AP} - R_P) / R_P$ ratio, fixed at 150 %) and taking into account the Gaussian distribution of the resistances R_{AP} and R_P (with a 10% of maximum variation). This technique enables the optimization of the sensing circuitry by unbalancing the reading transistors to achieve a 100 % detection accuracy and reliability on the output node 'out', without false positive sensing result, as illustrated in Figure 8.b.

In fact, illustrated results in Figure 8.a and Figure 8.b are performed using the same MC parameters but with different M_{nRd1} and M_{nRd2} transistors W/L ratio. They are equivalent in the first case (Figure 8.a), and unbalanced in the second case (as established in subsection III.C and illustrated in Figure 8.b). Thus, for the integration of the STT-MRAM technology in the sensor landscape, MC simulations are mandatory in order to confirm the circuit operation in different conditions.

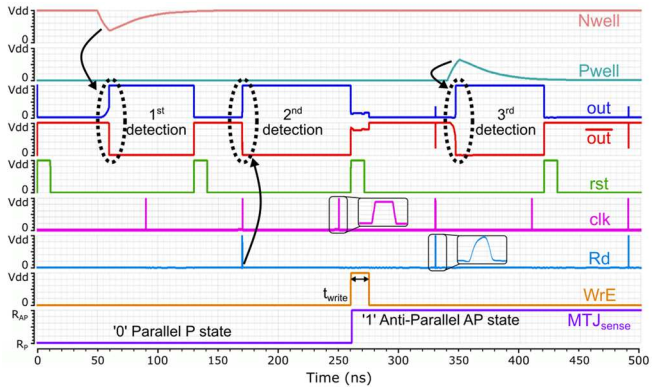


Figure 7: Simulation of the proposed dual sensing architecture. The structure detects three types of attacks respectively: an induced current in the "Nwell", a resistance modification of the MTJ_{sense} and an induced current in the "Pwell". After each detection, the structure is reset.

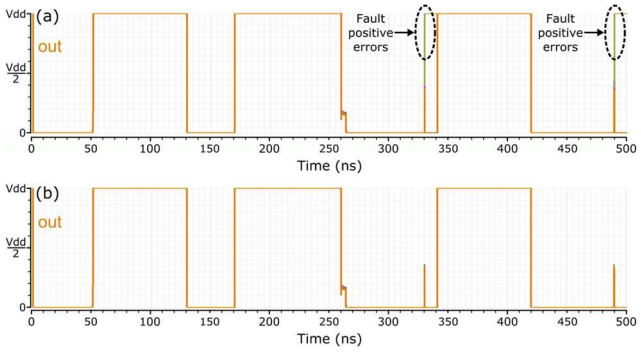


Figure 8: 1,000 rounds Monte Carlo simulation of the DDHP. a) Simulation with 5% of errors. b) Optimisation of the sensing operation of the MTJs - no errors.

~~2)~~3) Area overhead of the proposed architecture

The proposed architecture is compared to the BBICS detector in terms of area. As specified in Figure 9, the proposed DDHP architecture requests a certain area overhead (6.4 Gate Equivalents) compared to a pure BBICS solution while introducing a countermeasure that performs a larger attack-sensing panel (bulk disturbance and emerging non-volatile memory perturbation).

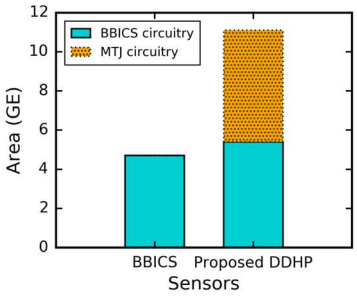


Figure 9: Area overhead represented in Gate Equivalents (GE) of the proposed DDHP architecture compared to a BBICS structure.

V. Conclusion and Perspectives

In the Internet of things (IoT) context for instance but not limited to it, the security of connected objects is a major challenge. The integrated circuits perturbation mainly induced by environmental radiations or malicious perturbations such as photoelectrical or thermal perturbations, becomes a huge concern for the circuits' development. Thus, embedding an external sensor enabling the notification of any threat demonstrated its interest in the security scenery. In this landscape, our work proposes an innovative detector to sense external malicious attacks that could be induced on CMOS or on STT-MRAM technologies. This sensor designated by Dual Detection of Heating and Photocurrent attacks (DDHP) requests a certain area overhead with a high security contribution (photoelectrical and thermal perturbations detected). This structure provides also the detection of attacks that may target the STT-MRAMs used as a reference. Moreover, Monte Carlo simulations demonstrated the excellent efficiency of this sensor by detecting 100 % of the malicious perturbations developed in this work and that could affect the circuit operation.

In order for the proposed detector to be efficient at the chip's level, the sensing junctions have to be multiplied to perform a sensing operation protecting the entire IC surface. In this context, an experimental work testing the scope of action in terms of area of a DDHP sensor must be led and an advanced DDHP structure proposed.

References

[1] R. A. Camponogara Viera, R. P. Bastos, J.-M. Dutertre, P. Maurine, and R. I. Jadue, 'Method for evaluation of transient-fault detection techniques', *Microelectronics Reliability*, vol. 76–77, no. Supplement C, pp. 68–74, Sep. 2017.

[2] T. Karnik and P. Hazucha, 'Characterization of soft errors caused by single event upsets in CMOS processes', *IEEE Transactions on Dependable and Secure Computing*, vol. 1, no. 2, pp. 128–143, Apr. 2004.

[3] C. H. Kim and J. Quisquater, 'Faults, Injection Methods, and Fault Attacks', *IEEE Design Test of Computers*, vol. 24, no. 6, pp. 544–545, Nov. 2007.

[4] S. P. Buchner, F. Miller, V. Pouget, and D. P. McMorrow, 'Pulsed-Laser Testing for Single-Event Effects Investigations', *IEEE Transactions on Nuclear Science*, vol. 60, no. 3, pp. 1852–1875, Jun. 2013.

[5] D. H. Habing, 'The Use of Lasers to Simulate Radiation-Induced Transients in Semiconductor Devices and Circuits', *IEEE Transactions on Nuclear Science*, vol. 12, no. 5, pp. 91–100, Oct. 1965.

[6] M. Chambonneau *et al.*, 'Suppressing the memory state of floating gate transistors with repeated femtosecond laser backside irradiations', *Appl. Phys. Lett.*, vol. 110, no. 16, p. 161112, Apr. 2017.

[7] J. M. Dutertre *et al.*, 'Improving the ability of Bulk Built-In Current Sensors to detect Single Event Effects by using triple-well CMOS', *Microelectronics Reliability*, vol. 54, no. 9, pp. 2289–2294, Sep. 2014.

[8] C. Champeix, N. Borrel, J. M. Dutertre, B. Robisson, M. Lisart, and A. Sarafianos, 'Experimental validation of a Bulk Built-In Current Sensor for detecting laser-induced currents', in *2015 IEEE 21st International On-Line Testing Symposium (IOLTS)*, pp. 150–155, 2015.

[9] E. H. Neto, I. Ribeiro, M. Vieira, G. Wirth, and F. L. Kastensmidt, 'Evaluating Fault Coverage of Bulk Built-in Current Sensor for Soft Errors in Combinational and Sequential Logic', in *2005 18th Symposium on Integrated Circuits and Systems Design*, pp. 62–67, 2005.

[10] E. H. Neto, I. Ribeiro, M. Vieira, G. Wirth, and F. L. Kastensmidt, 'Using Bulk Built-in Current Sensors to Detect Soft Errors', *IEEE Micro*, vol. 26, no. 5, pp. 10–18, Sep. 2006.

[11] '2013 International Technology Roadmap for Semiconductors (ITRS)', *Semiconductor Industry Association, 2013*. .

[12] A. Krakovinsky, M. Bocquet, R. Wacquez, J. Coignus, and J. M. Portal, 'Thermal laser attack and high temperature heating on HfO2-based OxRAM cells', in *2017 IEEE 23rd International Symposium on On-Line Testing and Robust System Design (IOLTS)*, pp. 85–89, 2017.

[13] M. Kharbouche-Harrari *et al.*, 'Impact of a Laser Pulse on a STT-MRAM Bitcell: Security and Reliability Issues', in *2018 IEEE 24th International Symposium on On-Line Testing And Robust System Design (IOLTS)*, pp. 243–244, 2018.

[14] J. Dutertre *et al.*, 'The case of using CMOS FD-SOI rather than CMOS bulk to harden ICs against laser attacks', in *2018 IEEE 24th International Symposium on On-Line Testing And Robust System Design (IOLTS)*, pp. 214–219, 2018.

[15] A. Barenghi, L. Breveglieri, I. Koren, and D. Naccache, 'Fault Injection Attacks on Cryptographic Devices: Theory, Practice, and Countermeasures', *Proceedings of the IEEE*, vol. 100, no. 11, pp. 3056–3076, Nov. 2012.

[16] S. Skorobogatov, 'Local heating attacks on Flash memory devices', in *2009 IEEE International Workshop on Hardware-Oriented Security and Trust*, pp. 1–6, 2009.

[17] D. Sands, 'Pulsed Laser Heating and Melting', in *Heat Transfer - Engineering Applications, Prof. Vyacheslav Vikhrenko (Ed.)*, 2011.

[18] F. S. Torres and R. P. Bastos, 'Robust modular Bulk Built-in Current Sensors for detection of transient faults', in *2012 25th Symposium on Integrated Circuits and Systems Design (SBCCI)*, pp. 1–6, 2012.

[19] J. M. Dutertre, R. Possamai Bastos, O. Potin, M. L. Flottes, B. Rouzeyre, and G. Di Natale, 'Sensitivity tuning of a bulk built-in current sensor for optimal transient-fault detection', *Microelectronics Reliability*, vol. 53, no. 9, pp. 1320–1324, Sep. 2013.

[20] A. Simionovski and G. Wirth, 'Simulation Evaluation of an Implemented Set of Complementary Bulk Built-In Current Sensors With Dynamic Storage Cell', *IEEE Transactions on Device and Materials Reliability*, vol. 14, no. 1, pp. 255–261, Mar. 2014.

[21] S. Senni, L. Torres, G. Sassatelli, A. Gamatie, and B. Mussard, 'Exploring MRAM Technologies for Energy Efficient Systems-On-Chip', *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 6, no. 3, pp. 279–292, Sep. 2016.

[22] S. Fukami, H. Sato, M. Yamanouchi, S. Ikeda, F. Matsukura, and H. Ohno, 'Advances in spintronics devices for microelectronics-from spin-transfer torque to spin-orbit torque', in *2014 19th Asia and South Pacific Design Automation Conference (ASP-DAC)*, pp. 684–691, 2014.

[23] Y. Huai, 'Spin-transfer torque MRAM (STT-MRAM): Challenges and prospects', *AAPPS*, vol. 18, 2008.