Resistance of Radiation Tolerant TMR Shift Registers to Optical Fault Injections

Dmytro Petryk[1], Peter Langendörfer[1,2] and Zoya Dyka[1,2]
[1] *IHP – Leibniz-Institut für innovative Mikroelektronik,* Frankfurt (Oder), Germany
[2] *BTU Cottbus-Senftenberg,* Cottbus, Germany
{petryk, langendoerfer, dyka}@ihp-microelectronics.com

Abstract—**Protection of information is essential for IoT devices. They are often subject to lab analysis with the objective to reveal secret hidden information. One of the ways to reveal the cryptographic key is to perform optical Fault Injection attacks. In this work, we investigated the IHP radiation tolerant shift registers built of Triple Modular Redundant flip-flops. In our experiments, we were able to inject different transient faults into TMR registers using a single laser beam.**

Keywords — Fault Injection attack, laser, reliability, security, triple modular redundancy, standard library, rad-hard flip-flops.

I. Introduction

Confidentiality, data integrity, availability of services, and (mutual) authentication of communicating devices are the main goals which have to be implemented to guarantee a secure communication of the devices. It is ensured by using cryptographic algorithms. Cryptographic protocols are based on the secrecy of the used keys. The goal of many attacks is to extract the private/secret key. The cryptographic approaches are based on complex mathematical problems, which cannot be solved in a reasonable time if the used private/secret key is long enough. This changes dramatically if an attacker has physical access to the attacked device. Physical parameters such as the execution time of cryptographic operations, current drawn from the power supply, electromagnetic radiation, etc., called side-channel effects, can be measured during the execution of cryptographic operations and later analysed using statistical methods, signal processing methods or machine learning methods. Practically, many cryptographic algorithms process a private key or a secret scalar bit-by-bit. Many attacks concentrate on the analysis of registers' activity. Some attacks exploit the key-dependent hamming weight of the data, stored in registers, and require usually many traces for the analysis [1]. Other attacks exploit the distinguishability of the registers addressing and can be successful when analysing many traces [2] as well as a single trace only [3], [4]. The sensitivity of cryptographic chips to the environmental and operating parameters – temperature, voltage, light, etc. – can be exploited to reveal the cryptographic key too. A fluctuation of these parameters can cause fault(s). Cryptographic keys can be revealed by analysing such faults. Due to this fact, IoT devices have to be resistant to a broad spectrum of physical attacks such as Side-Channel Attacks (SCA) & Fault Injection (FI) attacks.

There are many different possibilities to increase the resistance against SCA attacks. The processed data can be hidden using different kinds of noise, or by applying randomization of inputs and the processing sequence. The main idea of the countermeasures is to make the measurable side-channel effects not dependable on the processed cryptographic key, or – at least – to reduce this dependability significantly. A common approach to increase resistance against FI attacks is to implement countermeasures based on redundancy techniques. The main idea of the countermeasures is to avoid successful manipulation of device parameters, or – at least – to reduce the influence of successful manipulations of the design.

In this work, we investigate the applicability of the radiation hard Triple Modular Redundancy (TMR) technique against optical FI attacks. Our first investigations were published in [24]. In this paper, we present a complete investigation of the resistance of radiation tolerant shift registers to optical FI attacks as well as provide the area of the investigated TMR flip-flops sensitive to laser illumination. The paper is structured as follows. Section II describes optical FI attacks, redundancy as a countermeasure against FI attacks and our previous works. Section III describes the attacked chip, our FI setup and attack scenarios. Section IV gives the results of our optical Fault Injection attacks against TMR shift registers. Section V concludes this work.

II. Optical Fault Injection Attacks

Optical FI attacks using lasers belong to the class of semi-invasive attacks and exploit the sensitivity of semiconductors to the visible light, i.e. internal photoelectric effect. This phenomenon describes the generation of "free" electrons in semi-conductor/dielectric material under light. A sufficient number of the additional "free" electrons generated in close vicinity to the transistor gate of the attacked closed transistor results in a current flow that can switch a transistor from the high resistance state to the low resistance state. If the attacked transistor changes its state from OFF to ON it can cause a change of the logic cell state. The pioneering work regarding optical FI attacks was published already in 2002 [5]. The attacks can be performed through the back-side (silicon) of the chip [22] or the front-side (metal layers) [17] or the lateral-side [25]. To implement the former, near-infrared (NIR) and infrared (IR) lasers are used. This is due to a low absorption of NIR and IR waves propagating through silicon [22]. The latter can be implemented with any kind of wavelength [17], but the optimal choice is a laser with 800 nm wavelength. An overview of FI attacks against implementations of cryptographic operations using elliptic curves, including laser-based attacks, is given in [19]. An overview of optical FI attacks against different cryptographic and non-cryptographic implementations as well as used equipment is given in [6]. An optical FI attack against secured microcontrollers is reported in [14]. A multi-fault laser attack on an RSA-CRT implementation is described in [15].

A. H/W redundancy as a countermeasure against faults

Hardware redundancy is one of the means to reduce the success of FI [18]. We concentrate here on the hardware redundancy, especially on the TMR technique implementing registers. So-called standard NMR and full NMR are well-known types of hardware redundancy circuit architectures [11]. The standard TMR architecture for storing a single bit of information is based on a triplication of the flip-flop and implementation of a voter. The full TMR architecture is based on the triplication of each cell, i.e. flip-flop (FF), voter and other combinational logic cells have to be triplicated. The weak point of the standard TMR architecture is its voter, due to the fact that a fault injected into the voter manipulates the output value of the TMR-FF. To prevent this issue a full-TMR architecture can be used. The triplication of the voter increases the power consumption and area overhead of the TMR-FF.

B. Our previous works

In our previous publications we described successful attacks against different standard logic cells manufactured in IHP's 250 nm as well as in IHP's 130 nm technologies. We were able to inject transient as well as permanent faults into inverter-, NAND-, NOR-cells and FFs [7], [8]. Additionally, we investigated the possibility to inject a fault (using a red laser) into Resistive Random Access Memory (RRAM) cells [16] and radiation hard Junction Isolated Common Gate (JICG) flip-flops [10]. TABLE I gives a short overview of our results.

TABLE I. OVERVIEW OF RESULTS OF OPTICAL FI ATTACKS AGAINST DIFFERENT CELLS MANUFACTURED IN IHP'S TECHNOLOGIES

Red laser	Technology, nm	Successfully attacked structures		
		Standard IHP library cells	**RRAM**	**JICG**
Single-mode	250	'1'→ '0' INV NOR NAND	(a) 0↔1, 0↔US, US↔1, 0↔Stuck-at 1, US↔Stuck-at 1, 1↔Stuck-at 1	'1'→'0'; '0'→'1'.
Multi-mode	130	'0'→ '1' FF	Not investigated yet	Not investigated yet

[a] SPECIFIC OF RRAM (4 DEFINED STATES [16]); US IS AN UNDEFINED STATE.

All our FI attacks were successful, even against radiation-hard JICG FF that utilizes duplication of non-standard transistors. These transistors are placed at a distance to ensure blocking capability against particle hit. Despite the implemented measures, we were able to illuminate a pair of duplicated transistors and manipulate the data stored. Details about successful attacks on JICG FFs can be found in [9], [23]. Since our attacks against the JICG flip-flops were successful we decided to evaluate the TMR technique available at IHP [20]. We experimented with shift registers that have been: designed to survive space missions, evaluated in single event effect measurements, verified as very radiation tolerant [21].

III. ATTACKED CHIP, OUR EXPERIMENTAL SETUP AND ATTACK SCENARIOS

A. IHP TMR shift register

We attacked radiation tolerant TMR shift registers designed at IHP and manufactured in IHP's CMOS 130 nm technology [21]. Two chips, each containing a single 1024-bit long TMR shift register, were bonded on a PCB, see **Fig. 1**. The attacked TMR circuit is based on the standard TMR architecture, i.e. there are 3072 flip-flops and 1024 voters, with two additional delay elements of 0.5 ns and 1.0 ns to filter possible transients at the inputs of the FFs, see **Fig. 2**. More details about the delay elements can be found in [21].

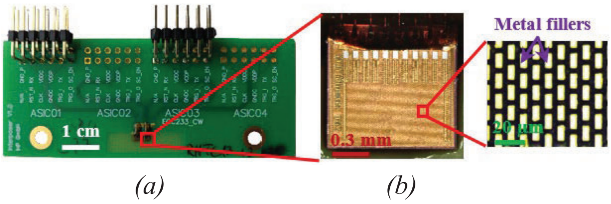

Fig. 1. The attacked chips: *(a)* – PCB with 2 TMR shift registers; *(b)* – a TMR shift register chip, zoomed in.

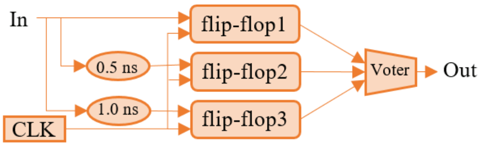

Fig. 2. Structure of the attacked TMR-FF.

B. FI setup and attack scenarios

In our experiments we used a setup that consists of: a modified Riscure Diode Laser Station (DLS), a VC glitcher, a PC with the Riscure Inspector software, a stable power supply, a signal generator and an oscilloscope. A detailed description of the experimental setup can be found in [23] and [23]. The original FI setup consists of a DLS that is equipped with two multi-mode lasers: a near-infrared (1064 nm) laser and a red (808 nm) laser [12], and with a single-mode laser from Alphanov [13]. In this work we applied the same equipment as in our experiments described in [7], [8] and [10]. The laser parameters, such as the laser pulse power and duration, were already evaluated experimentally in [23]. This allows to compare all our FI attack results.

In our experiments, we sent a constant input ('1' or '0') to the attacked shift register during the whole time of the experiment. We performed our experiments applying two clock signal frequencies: 10 MHz and 50 MHz. We performed attacks from the front-side since the decapsulation was not required. The placement of triplicated FFs in the layout of the attacked circuit is shown in **Fig. 3**. A triplicated flip-flop and its voter are placed in one row. The FFs are placed at different distances from each other. This distance reduces the probability of a fault occurrence caused by high energy particles due to the fact that at least two of FFs have to be influenced simultaneously. Due to the placement of the cells in the TMR-FF layout, we have three possible attack scenarios:

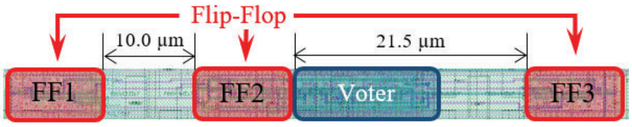

Fig. 3. Layout of the TMR-FF attacked.

Scenario1: attack illuminating logic cells of the voter.
Scenario2: attack illuminating FF1 and FF2 simultaneously.
Scenario3: attack illuminating the whole TMR-FF, i.e. illuminating three FFs and the voters simultaneously.

The issue is that during the attack according to *Scenario3* multi-faults can be injected. It can cause the "attack failed" case. For example, if faults are injected into two (or into all three) FFs and an additional fault is injected into the voter, the output of the TMR-FF will be equal to its fault-free state. Please note that additional difficulties in our experiments arise due to the so-called metal fillers. The metal fillers are small metal areas that are placed in different metal layers between the connection wires to maintain homogeneity of the etching process during manufacturing. Due to the metal fillers, the internal structure of the attacked TMR shift register is not visible through a microscope from the front-side, see **Fig. 1**. Nevertheless, in our previous experiments with the IHP standard logic cells we were able to induce faults successfully despite inserted metal fillers. Due to the fact that cells are unevenly covered by metal fillers, we expected that not all TMR-FFs will be successfully influenced.

IV. Experiments and Results

We performed our experiments according to *Scenario1* and *Scenario2* only, due to the difficulties of Scenario3 described above. We illuminated the last TMR-FF of the register first. Additionally, we attacked other randomly selected TMR-FFs.

Scenario1: We started our experiments using the single-mode red laser. The attacked register was clocked with a frequency of 10 MHz, i.e. the clock signal period is 100 ns. We started with 10 % laser power and 130[1] ns pulse duration using a 50× objective. We applied a 0.5 µm step size for the X- and Y-axis for the scanning of the voters' area. If we did not observe a fault during a scan of the whole area of the voter, we increased laser beam power stepwise up to 100 % and/or pulse duration up to 280 ns. After the experiments with the 50× objective we switched to the 100× objective and performed similar experiments. We did not observe a fault injection into the attacked TMR-FF. We attacked additional 34 TMR-FFs. All attacks were unsuccessful. Our experiments with the same laser parameters but with the clock frequency of 50 MHz[2], were not successful as well.

We also performed experiments using the more powerful multi-mode red laser. We started the experiments with 50 % laser beam power. All other parameters – the pulse duration, objective, etc. – were applied as for the experiments described above. After we reached the "maximum" parameter values, we switched to 100× objective and performed similar experiments. We attacked 24 TMR-FFs in total, but we did not observe a fault injection. We expected successful attacks using the multi-mode laser since we were able to influence standard library cells manufactured in IHP's 130 nm technology with metal fillers [8]. Nevertheless, all our FI attacks illuminating the voter of different FFs were not successful. It can be explained due to the difference regarding laser parameters between experiments described in [8] and here: in previous work we used a standard DLS from Riscure, after then the DLS was modified to allow using the Alphanov single-mode laser. We assume that the modification reduced the laser beam power.

Scenario2: In this attack scenario, we used the multi-mode laser to influence both FFs simultaneously. We started with 40 % power, 130 ns pulse duration, 20× objective and 1 µm step size for the X- and Y-axis. The register was clocked with a frequency of 10 MHz. We observed repeatedly successful bit-set ('0'→'1') and bit-reset ('1'→'0') faults. **Fig. 4** shows waveform of the measured signals demonstrating bit-reset fault into the last TMR-FF of the attacked TMR shift register.

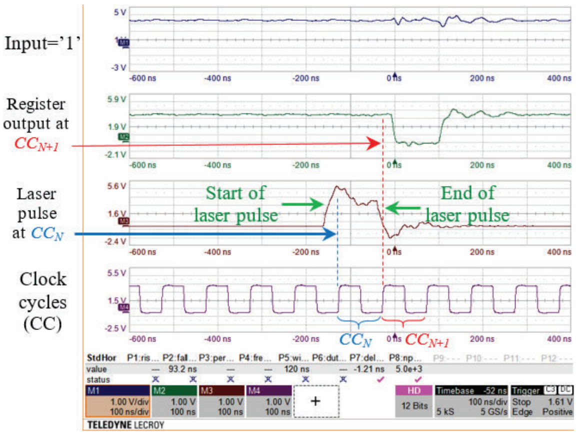

Fig. 4. Oscilloscope waveforms of laser pulse, clock, input and output of the attacked shift register measured demonstrating successful *bit-reset* fault into the last flip-flop.

Afterwards we performed similar experiments with a 5× objective and observed successful faults also. We attacked 24 TMR-FFs in total, of which 10 TMR-FFs were manipulated.

We also performed experiments with an increased laser power (up to 100%) and pulse duration (up to 280 ns) to assess the influence on the behaviour of the register. Neither *permanent*[3] nor *stuck-at*[4] faults were observed, even when applying maximum laser beam power. After the performed experiments, the register is fully functional, i.e. its

[1] We obtained this minimal pulse duration as a sum of the rise time of the single-mode laser to reach its peak power [13] and the clock signal period, i.e. 30 ns+100 ns=130 ns. The maximal pulse duration is as a sum of the rise time and the duration of 2.5 clock signal periods that results into 30 ns+2.5*100 ns=280 ns.

[2] We started with the pulse duration of 30 ns+20 ns=50 ns and increased it up to 30 ns+2.5*20 ns=80 ns.

[3] change of logic state is no more possible.

[4] change of logic state cannot be changed before the device shutdown.

surface is intact and the internal structure of the chip was not damaged. TABLE II gives an overview of our successful optical FI attacks against the IHP TMR registers for the *Scenario2*.

TABLE II. RESULTS OF ATTACKS AGAINST THE TMR REGISTERS

Register clock frequency, MHz	Register input	Magnification objective	Power, %[a]	Pulse, ns	Type of fault
50	'0'	20×	80-100	80	*bit-set*[b]
	'1'		90-100	50-80	*bit-reset*
	'0'	5×	90-100		*bit-set*
	'1'		60-100		*bit-reset*
10	'0'	20×	40-100	130-280	*bit-set*
	'1'		45-100		*bit-reset*
	'0'	5×	65-100		*bit-set*
	'1'		55-100		*bit-reset*

[a] POWER MEASUREMENT UNIT IN RISCURE SOFTWARE [12]. THE FIRST VALUE IN THE COLUMN "POWER" REPRESENTS THE MINIMAL POWER THAT RESULTS IN REPEATABLE FAULTS.

[b] THE FAULT IS NOT FULLY REPEATABLE.

According to the TMR shift register's layout, we observed successful FIs when the centre of a laser beam spot was over area marked yellow in **Fig. 5**. Due to the unknown profile of the laser beam intensity distribution of the used multi-mode laser and the fact that our precisely localised attacks on the voter (*Scenario1*) failed, we assume that faults were successfully injected in two adjacent FFs in the TMR-FF. Nevertheless, we do not exclude the fact that faults could be injected in each pair or even into three FFs simultaneously using the 5× objective since the laser beam spot allows to cover the whole TMR-FF.

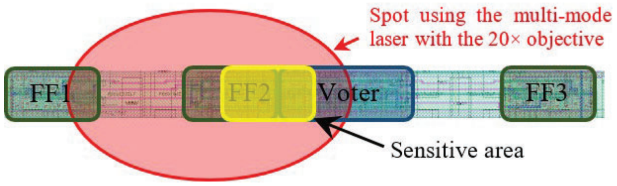

Fig. 5. Sensitive areas in the attacked TMR-FF.

V. CONCLUSION

In this work, we investigated the vulnerability of IHP radiation tolerant TMR-registers based on standard library flip-flops manufactured in 130 nm technology against front-side optical FI attacks. We performed attacks against the voter (*Scenario1*) and the triplicated FFs (*Scenario2*). We performed attacks using the Alphanov's single-mode red laser as well as the Riscure's multi-mode red laser. Attacks against voters were unsuccessful. Performing attacks against FFs we were able to inject transient repeatable *bit-set* as well as *bit-reset* faults into the IHP TMR shift registers using the multi-mode laser.

REFERENCES

[1] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis", in Advances in Cryptology — CRYPTO' 99, vol. 1666, Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, pp. 388–397.

[2] K. Itoh, T. Izu, and M. Takenaka, "Address-Bit Differential Power Analysis of Cryptographic Schemes OK-ECDH and OK-ECDSA", in Cryptographic Hardware and Embedded Systems, 2002, pp. 129–143.

[3] I. Kabin, Z. Dyka, D. Klann, and P. Langendoerfer, "Methods increasing inherent resistance of ECC designs against horizontal attacks", Integration, vol. 73, Jul. 2020, pp. 50–67.

[4] I. Kabin, Z. Dyka, and P. Langendoerfer, "Atomicity and Regularity Principles Do Not Ensure Full Resistance of ECC Designs against Single-Trace Attacks", Sensors, vol. 22, no. 8, Art. no. 8, Jan. 2022.

[5] S. Skorobogatov and R. Anderson, "Optical Fault Induction Attacks", Workshop on Cryptographic Hardware and Embedded Systems (CHES), USA, San Francisco, Aug, 13–15, 2002, pp. 2–12.

[6] D. Petryk et al., "Optical Fault Injections: a Setup Comparison", Proc. PhD Forum of the 8th BELAS Summer School, Estonia, Tallinn, June 20–22, 2018, pp. 1–5.

[7] D. Petryk, Z. Dyka and P. Langendörfer, "Sensitivity of Standard Library Cells to Optical Fault Injection Attacks in IHP 250 nm Technology", 2020 9th Mediterranean Conference on Embedded Computing (MECO), Montenegro, Budva, June 8–11, 2020, pp. 1–4.

[8] D. Petryk, Z. Dyka, J. Katzer and P. Langendörfer, "Metal Fillers as Potential Low Cost Countermeasure against Optical Fault Injection Attacks", 2020 IEEE East-West Design & Test Symposium (EWDTS), Bulgaria, Varna, Sept. 4–7, 2020, pp. 1–6.

[9] R. Sorge et al., "JICG MOS transistors for reduction of radiation effects in CMOS electronics", 2018 IEEE Topical Workshop on Internet of Space (TWIOS), USA, CA, Anaheim, Jan. 14–17, 2018, pp. 17–19.

[10] D. Petryk et al., "Optical Fault Injection Attacks against Radiation-Hard Shift Registers", 2021 24th Euromicro Conference on Digital System Design (DSD), Italy, Palermo, Sept. 1–3, 2021, pp. 371–375.

[11] V. Petrovic and M. Krstic, "Design Flow for Radhard TMR Flip-Flops", 2015 IEEE 18th International Symposium on Design and Diagnostics of Electronic Circuits & Systems (DDECS), 2015, pp. 203–208.

[12] Riscure. Diode Laser Station Datasheet, 2011. https://www.riscure.com/security-tools/inspector-hardware/

[13] Alphanov PDM laser sources. Rise time comparison. URL: https://www.alphanov.com/en/products-services/pdm-laser-sources

[14] Jasper G. J. van Woudenberg et al., "Practical optical fault injection on secure microcontrollers", 2011 Workshop on Fault Diagnosis and Tolerance in Cryptography, Japan, Nara, Sept. 28, 2011, pp. 91–99.

[15] E. Trichina and R. Korkikyan, "Multi Fault Laser Attacks on Protected CRT-RSA", 2010 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC), USA, CA, Aug. 21, 2010, pp. 75–86.

[16] D. Petryk et al., "Sensitivity of HfO2-based RRAM Cells to Laser Irradiation", Microprocessors and Microsystems, Volume 87, 2021, 104376, ISSN 0141-9331, pp. 1–20.

[17] S. de Castro et al., "Frontside Versus Backside Laser Injection: A Comparative Study", ACM Journal on Emerging Technologies in Computing Systems, 2016, 13 (1), pp. 7.

[18] M. Krstic, "Optimizing Design of Fault-Tolerant Computing Systems", Workshop on Hardware Design and Theory, Austria, Vienna, 2017.

[19] J. Fan et al., "State-of-the-art of secure ECC implementations: a survey on known side-channel attacks and countermeasures", 2010 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), USA, CA, Anaheim, 2010, pp. 76-87.

[20] IHP – Leibniz-Institut für innovative Mikroelektronik. URL: https://www.ihp-microelectronics.com/about-us

[21] O. Schrape et al., "Design and Evaluation of Radiation-Hardened Standard Cell Flip-Flops", in IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 68, no. 11, Nov. 2021, pp. 4796-4809.

[22] D. Lewis et al., "Backside Laser Testing of ICs for SET Sensitivity Evaluation", IEEE Transactions On Nuclear Science, Vol. 48, No. 6, Dec. 2001, pp. 2193-2201.

[23] D. Petryk, "Investigation of sensitivity of different logic and memory cells to Laser Fault Injections", Doctoral thesis, BTU Cottbus – Senftenberg, 2024. DOI: 10.26127/BTUOpen-6664

[24] D. Petryk et al., "Laser Fault Injection Attacks against Radiation Tolerant TMR Registers", 2022 IEEE 23rd Latin American Test Symposium (LATS), Montevideo, Uruguay, 2022, pp. 1-2.

[25] J. Rodriguez, A. Baldomero, V. Montilla and J. Mujal, "LLFI: Lateral Laser Fault Injection Attack", 2019 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC), Atlanta, USA, 2019, pp. 41-47.