Optical Fault Injection Attacks against Different Logic and Memory Cells

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

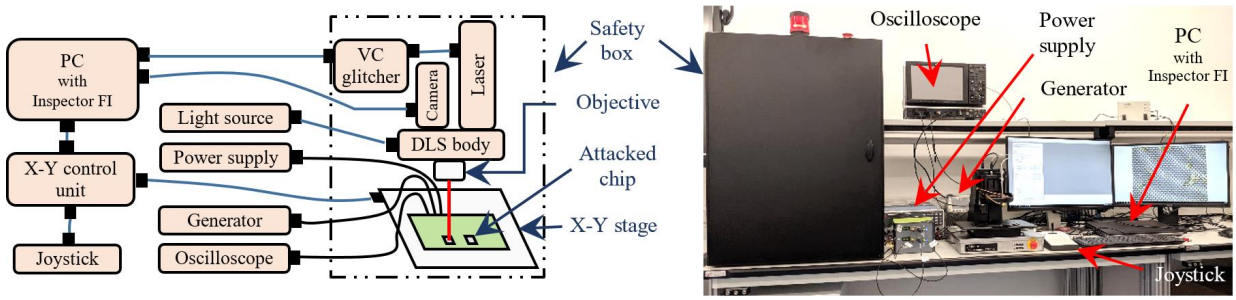
Semiconductor devices are widely used for industrial control systems, smart cities, battery powered devices for e-health, the Internet of Things, etc. Plenty of the devices are developed to operate with private data, i.e. the data processed and stored in them have to be protected from the malicious users. The crucial security requirements for such devices are confidentiality, data integrity, authentication, services availability, authenticity and non-repudiation. To guarantee them cryptographic algorithms are used, where the secrecy is based on the secrecy of the private/secret keys. From mathematical point of view these algorithms using keys with recommended lengths are secure. The issue is that usually physical access the devices can be gained, i.e. a potential attacker can steal and attack them in a specialized lab. Practically, many physical attacks are aimed to extract cryptographic keys or cause data leakage and are much more effective than brute force.

Some physical attacks exploit the fact that different cryptographic operations performed consume different power and also depend on the cryptographic key processed. To realize the attack an attacker can measures the so-called side-channel effects during a cryptographic operation, e.g. current drawn from the power supply, electromagnetic radiation, execution time, etc. The measured data can be then analysed using statistical, machine learning or artificial intelligence methods with the goal to reveal the key. Such attacks are known as Side-Channel Analysis (SCA) attacks. Other class of physical attacks are different manipulations exploiting the sensitivity of semiconductor devices to their environmental and working parameters: temperature, operating voltage, frequency, electromagnetic pulses, light, and so on. The goal of an attacker is to inject the faults that cause incorrect output of cryptographic operations. The used cryptographic key can be revealed analysing the incorrect outputs. These attacks are known as Fault Injection (FI) attacks. In practice, both types of attacks are effective means to compromise the device security. This work focuses on the attacks using laser as the light source to inject fault into logic and memory cells.

The attacks exploit the sensitivity of semiconductor devices to the visible light. For example, illuminating a transistor it is possible to switch it from a high resistance state to a low resistance state. The use of laser to inject faults into semiconductor devices was firstly introduced in 1965 [1]. Attacks using lasers belong to the semi-invasive class, i.e. it requires to perform a chip decapsulation. They can be performed through a back-side (silicon) of the chip or its front-side (metal layers). To implement back-side attacks, near-infrared (NIR) and infrared (IR) lasers are usually used. This is due to a low absorption of NIR and IR waves propagating through silicon, i.e. silicon is "transparent" to these wavelengths. The front-side attacks can be implemented with any kind of wavelength, but the optimal choice is a laser with 800 nm wavelength. To implement optical FI attack effectively various parameters should be considered, e.g. laser parameters: wavelength, its spot size, intensity and pulse duration.

Practical successful FI attacks against RSA cryptographic operations executed on a smartcard was presented in 2002 [2]. Since then various cryptographic implementations have been attacked. The overview of the optical FI attacks performed against different cryptographic algorithms as well as different cells and memories can be found in [3]. In the literature, majority of the attacks were performed through the back-side of the chip. This works reports on successful front-side optical FI attacks.

We performed the attacks using the setup available at IHP. It consists of: a 1st generation Riscure Diode Laser Station (DLS), a PC with the Riscure Inspector FI software, a stable power supply, a generator and an oscilloscope. The setup is shown schematically in Fig. 1.



(a) *(b)*

Fig. 1. Optical fault injection setup: *(a)* – a schematic view; *(b)* – the setup in IHP laboratory.

The setup can be used with three lasers: a red 808 nm single-mode laser from Alphanov, a red 808 nm and a NIR 1064 nm multi-mode lasers from Riscure. The front-side optical FI attacks were performed using the red single-mode and the red multi-mode lasers. Details about the setup parameters attacking different logic and memory cells can be found in [5]-[10].

The DLS is controlled by the Riscure software. The interaction between devices of the setup is automated by Riscure and users do not have access to it. Some parameters in the software used to perform attacks are represented in the Riscure-defined units, which are not the generally known units such as meters, seconds, etc. Clear rules for the unit conversion are not given. Thus, to ensure the repeatability of the experimental results and compliance with the promoted specifications the parameters of the setup controlled by the Riscure Inspector FI software were evaluated. The results show that evaluated minimal movement speed and minimum step size of X-Y stage, laser beam spot sizes, as well as signal controlling laser beam pulse duration differ from the values given in the corresponding documents. The non-compliance of the parameters can influence the success and the repeatability of FI attacks significantly. The knowledge about the limitations is helpful for attack planning.

The chips attacked were manufactured in two technologies: in the 130 nm and in the 250 nm IHP technology [4]. The back-end-of-line offers 3 thin metal layers and 2 thick metal layers in the 250 nm technology; and 5 thin metal layers and 2 thick metal layers in the 130 nm technology. Due to the technology requirements, the chips manufactured at IHP have metal fillers. The metal fillers are small metal areas that are placed in different metal layers between the connection wires if the required metal density of the layer is not met. Metal fillers above the cells act as obstacles for a visual inspection, i.e. they hide the internal structure of a chip and cause difficulties illuminating the cell.

1) Chips based on standard library cells

Attacks were performed against chips manufactured in the IHP's 250 nm (SG25H3) technology further denoted as Libval025 and in the IHP's 130 nm (SG13G2) technology further denoted as Libval013 [4]. The Libval025 chips were manufactured in an "old" IHP technology without metal fillers. Thus, the internal structure of the chip is clearly visible through the front-side. The Libval013 chips were manufactured in a recent IHP's technology with metal fillers. Fig. 2 shows the front-side of *(a)* Libval025 and *(b)* Libval013 captured using a microscope camera and *(c)* their structural scheme.

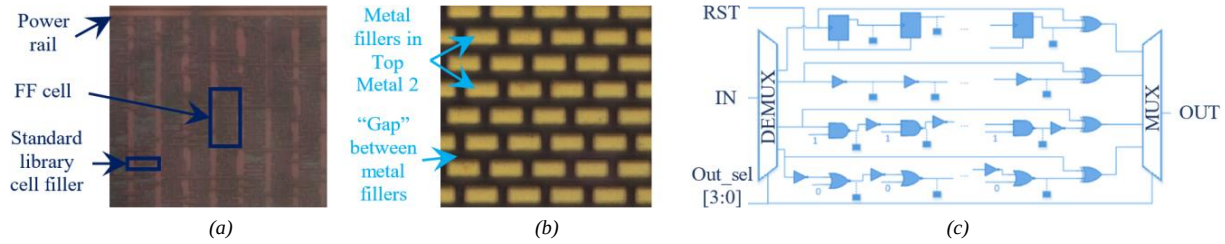


Fig. 2. Libval chip: *(a)* – front-side of Libval025; *(b)* – front-side of Libval013; *(b)* – structural scheme.

Originally the Libval chips were designed to measure signal propagation delays through chains of inverter, NAND, NOR and flip-flop cells. To perform laser attacks the chips were placed onto Printed Circuit Board (PCB). The PCB was placed on the X-Y stage.

The attacks against Libval chips were successful in a sense that repeatable faults were injected in all 4 types of gates, i.e. flip-flop, inverter, NOR and NAND cells. According to the input of the cells the following transient faults were successfully injected: *bit-reset* ('1'→'0') faults attacking inverter, NOR and NAND cells and *bit-set* ('0'→'1') faults attacking flip-flop cells. The Libval chips manufactured in the IHP's 250 nm were successfully attacked using both red lasers. The Libval chips manufactured in the IHP's 130 nm were successfully attacked using only the red multi-mode laser. Due to the metal fillers atop the cells in Libval013 the number of successfully influenced cells is significantly reduced compared to the number of successfully influenced cells in Libval025. Using the red multi-mode laser with the increased laser beam power permanent *stuck-at* faults were injected into inverter, NAND, NOR and flip-flop cells of Libval025 chip. Details of attacks against Libval chips can be found in [5] and [10].

According to the layout of the cells, coordinates taken from Riscure Inspector FI software and visual observations the areas of the attacked cells, which are sensitive to optical FI attacks, were determined. The injection of faults into logic cells of Libval chips, i.e. inverter, NAND, NOR and flip-flop cells, based on 250 nm technology was feasible illuminating area where NMOS transistors are placed.

2) Shift registers with applied radiation-hardening technique

Attacks were performed against shift registers with hardware redundancy. Hardware redundancy is widely considered as an effective measure to increase robustness of device developed for use in harsh environments. Devices/designs with hardware redundancy are often denoted as radiation-hard. Shift registers based on two radiation-hard techniques were attacked.

2.1) Shift registers based on Junction Isolated Common Gate (JICG) technique

JICG technique was designed to improve total ionizing dose and to prevent single event upsets. To improve the total ionizing dose the silicide blockers are used to realize Junction Isolation (JI) of the transistor drain-source region. To prevent single event upsets the transistors are doubled. Each NMOS and PMOS transistor in a CMOS circuit is substituted by two corresponding transistors. The gates of the transistor are connected, i.e. they have a common gate (CG). To maintain a blocking capability of duplicated transistors they are placed at a distance D_{DR}. Each chip is a 256-bit long register, i.e. it has 256 flip-flop cells connected in series. Single flip-flop cell consists of 6 NAND cells: 2 three-input and 4 two-input NAND cells, see cells marked C+*number* in Fig. 3. Each NAND cell is based on Inverter cells, i.e. CMOS circuits, to which JICG technique is applied.

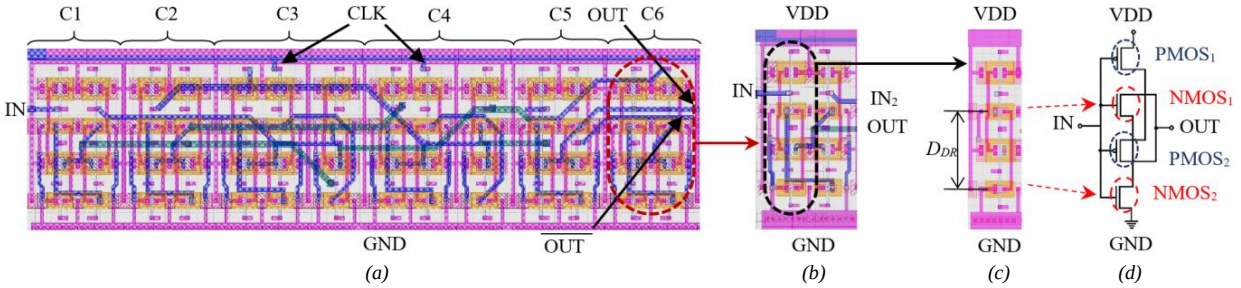


Fig. 3. JICG cells: *(a)* – layout of JICG flip-flop; *(b)* – layout of two-input JICG NAND cell; *(c)* –layout of JICG inverter; *(d)* – an electric circuit of JICG inverter.

The JICG shift registers attacked were manufactured in the IHP's 250 nm technology (SGB25RH) with metal fillers and placed in package with a window. To perform laser attacks the chips were placed on the X-Y stage.

To influence the state of the flip-flop two redundant transistors have to be manipulated simultaneously. To target redundant transistors the attacks were performed applying a single laser source, i.e. it was not a multi laser attack. The "large" laser beam spot size applied in our attacks covered both redundant transistors simultaneously. According to the active input of the register, transient *bit-set* and *bit-reset* faults were successfully injected using the red single-mode laser as well as the red multi-mode laser. Performing attacks with laser beam spot sizes that do not cover two redundant transistors simultaneously were unsuccessful. No permanent faults were observed applying even maximum configurable laser beam power and pulse duration.

The injection of faults into JICG flip-flops was feasible into its NAND cells with "closed" PMOS transistors, i.e. not all NAND cells of the attacked JICG flop-flops were sensitive to the laser illumination. Depending on the logic input of the JICG flip-flop different NAND cells were sensitive to the laser illumination. Attacks details against JICG registers can be found in [6].

2.2) Shift registers based on Triple Modular Redundancy (TMR) technique

The attacked TMR shift registers have been originally designed at IHP for use in space and manufactured in the IHP's 130 nm technology with metal fillers. Each manufactured chip is a 1024-bit long register where standard TMR architecture is applied for each bit, i.e. each chip has 3072 flip-flops and 1024 majority voters. The implementation attacked also has additional delay elements δ to filter short transients. Fig. 4 show *(a)* a block diagram of the part of the circuit containing 1 bit (TMR flip-flop) and *(b)* its layout.

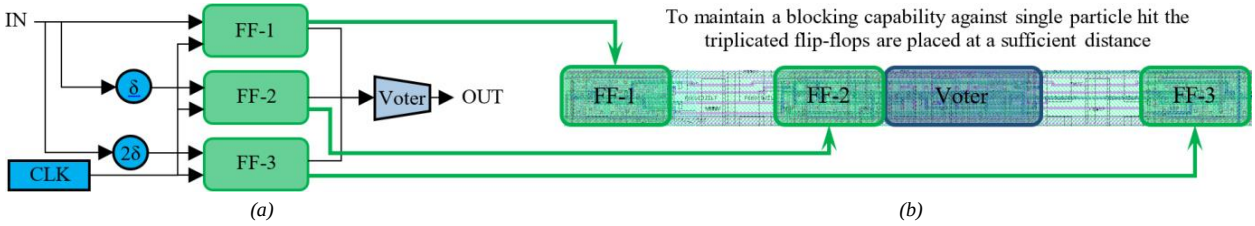


Fig. 4. The cell containing a bit in a TMR shift register: *(a)* – block diagram; *(b)* – layout of the cell.

To implement front-side FI attacks the chips were bonded to PCB. The PCB was placed on the X-Y stage. Attacks with small laser beam spot sizes, i.e. smaller than the distance between any two flip-flop cells, targeted at voter were unsuccessful using both lasers. Attacks with laser beam spot sizes covering at least two redundant flip-flop cells were successful. According to the active input of the register, transient *bit-set* and *bit-reset* faults were successfully injected using only the red multi-mode laser. Applying maximum configurable laser beam power and pulse duration no permanent faults were observed.

The injection of faults was feasible only when illuminating small area where flip-flop FF-2 and the voter is located. Due to the metal fillers above the TMR flip-flop as well as large laser beam spot size with unknown intensity distribution used to inject faults, it is not possible to clearly state what part of the TMR flip-flop was successfully influenced: voter or two redundant flip-flop cells. Due to the fact that attacks with small laser beam spot sizes targeted at voter were unsuccessful it is assumed that the manipulation was feasible by simultaneous influence on two flip-flops. Attack details against TMR registers can be found in [7].

3) Chips based on Resistive Random Access Memory (RRAM)

Due to the ability of RRAM to store data when the power is off, i.e. non-volatility, it is of interest to realize cryptographic devices. Nevertheless, for proper data protection the RRAM cells themselves should be resistant against external malicious influence, but it is rarely investigated compared to CMOS-devices.

The IHP RRAM chips attacked were manufactured in the IHP's 250 nm technology with metal fillers using standard library cells. Each chip contains 4 kbit of memory, i.e. it has 4096 RRAM cells. Each cell is based on 1 Transistor 1 Resistor

architecture, i.e. it has a transistor and a Metal-Insulator-Metal (MIM) structure. The goal of the attacks was to manipulate the state of the RRAM cell when no voltages are applied, i.e. standalone ships. To manipulate the state of RRAM cell we illuminated its MIM structure.

Manipulation of logic states of RRAM cells was feasible using both red lasers. Under the laser illumination the cells can change their logic state from the highest to the lowest one bypassing intermediate logic states. The new logic state of the attacked cell is not a transient one but will be stored in the cell. In the experiments, not only the RRAM cells illuminated directly with the laser beam, i.e. cells with gaps between metal fillers atop, but also the cells covered with metal fillers were successfully influenced. The reason of the attack success may be the well-known sensitivity of the RRAMs to temperature fluctuations. In this case the performed laser attack is a kind of a localized heating attack. To be able to use the metal fillers as a kind of countermeasure their form, placement and distribution in different metal layers have to contribute to heat dissipation. This assumption needs to be evaluated in the future. Details of attacks against IHP RRAM chips can be found in [8] and [9].

Generally, all the chips attacked in this work were successfully influenced. To prevent laser manipulations effective countermeasures have to be implemented. For example, metal fillers can be applied as optical obstacles reducing the success of front-side fault injection attacks. Based on the knowledge of the sensitive cell areas, the placement of the metal fillers can be automated in the future, i.e. the findings given in the work can serve as a basis for developing a methodology that allows to improve resistance against optical FI attacks already in the initial stage of chip development. Such methodology can be adapted for different chip manufacturing technology.

ACKNOWLEDGMENT

The work was partially done in the frame of RESCUE project. 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.

PAPER ORIGIN

This abstract is based on the following publications: [3], [5]-[10].

REFERENCES

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

[2] 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.

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

[4] IHP Technologies for MPW & Prototyping. URL: https://www.ihp-microelectronics.com/services/research-and-prototyping-service/mpw-prototyping-service/sigec-bicmos-technologies

[5] 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.

[6] D. Petryk, Z. Dyka, R. Sorge, J. Schäffner and P. Langendörfer, "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.

[7] D. Petryk, Z. Dyka, I. Kabin, A. Breitenreiter, J. Schäffner and M. Krstic, "Laser Fault Injection Attacks against Radiation Tolerant TMR Registers", 2022 IEEE 23rd Latin American Test Symposium (LATS), Uruguay, Montevideo, Sept. 5-8, 2022, pp. 1-2.

[8] D. Petryk, Z. Dyka, E. Perez, I. Kabin, J. Katzer, J. Schäffner and P. Langendörfer, "Sensitivity of HfO_2-based RRAM Cells to Laser Irradiation", Microprocessors and Microsystems, Volume 87, 2021, 104376, ISSN 0141-9331, pp. 1–20.

[9] D. Petryk, Z. Dyka, E. Perez, M. K. Mahadevaiaha, I. Kabin, Ch. Wenger and P. Langendörfer, "Evaluation of the Sensitivity of RRAM Cells to Optical Fault Injection Attacks", 23rd Euromicro Conference on Digital System Design (DSD), Kranj, Slovenia, 2020, pp. 238-245.

[10] 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.