Laser Fault Injection Attacks against IHP Rad-Hard Techniques

Dmytro Petryk Zoya Dyka

IHP – Leibniz-Institut für innovative Mikroelektronik
Frankfurt (Oder), Germany

34th Crypto Day, 9/10 June 2022

Cryptographic protocols are a means to achieve the main security goals: confidentiality, data integrity, services availability, etc. Private cryptographic keys have to be kept secret. The goal of many attacks is to reveal the private/secret keys. Cryptographic keys can be revealed by analysing faults, injected by attackers, whereby the mostly attacked blocks of cryptographic designs are the registers, for example the controller carrying out the operations and data flow [1]. A common approach to increase the resistance against FI attacks is to implement countermeasures based on redundancy techniques. Manipulation-critical registers can be implemented using a Triple Modular Redundancy (TMR) technique.

By fault injection attacks the sensitivity of semiconductor devices to the environmental and operating parameters such as temperature, voltage, frequency, light, EM pulses, radiation, etc. is exploited. Rad-hard designs developed for use in space are proved to be more robust against disturbances caused by particles and short electromagnetic waves compared to standard designs, i.e. designs based on non-rad-hard cells. Hence, rad-hard designs with enhanced fault tolerance seems to be very attractive option to improve resistance against physical attacks, e.g. laser-based FI attacks. However, their resistant has to be evaluated. IHP offers two radiation-hardening techniques including Junction Isolated Common Gate (JICG) and TMR. The JICG is based on custom transistor duplication and the TMR – on tripling critical cell/gate. In our previous works we have successfully attacked standard library cells (inverter, Flip-Flop (FF), NOR-, NAND- gates) [3], [4]. This work gives an overview of our successful attacks against IHP shift registers based on JICG- as well as TMR-technique against front-side optical FI attacks. Both types of registers had been originally designed for space application and manufactured at IHP [6]. To prevent faults redundant elements are placed at different distances from each other in both types of registers. Hence, large laser beam spots have to be used to inject the same kind of faults simultaneously in the redundant gate parts. To attack the shift registers we used a modified Riscure Diode Laser Station. The attacks were performed using a single-mode red laser from Alphanov and a multi-mode red laser from Riscure. Our attacks against shift registers were successful in a sense that we were able to manipulate their states.

crypto day matters 34 (2022)
Beiträge vom 34. Kryptotag, 09.-10. Juni 2022, online.
doi:10.18420/cdm-2022-34-05

We were able to inject transient and repeatable bit-set ('0' → '1') and bit-reset ('1' → '0') faults into both types of registers. Details about fault injection setup can be found in [2] and [5]. Our results clearly show that the rad-hard registers are still vulnerable to optical FI attacks despite significantly improved fault tolerance to radiation, i.e. resistance of such designs against malicious attacks is still not guaranteed.

References

[1] Ievgen Kabin, Zoya Dyka, Dan Klann & Peter Langendörfer (2020). Methods increasing inherent resistance of ECC designs against horizontal attacks. *Integration* **73**, 50–67. ISSN 0167-9260.

[2] Dmytro Petryk, Zoya Dyka, Ievgen Kabin, Anselm Breitenreiter, Jan Schäffner & Milos Krstic (2022). Laser Fault Injection Attacks against Radiation Tolerant TMR Registers. *Submitted to 2022 23RD IEEE LATIN-AMERICAN TEST SYMPOSIUM (LATS)* .

[3] Dmytro Petryk, Zoya Dyka, Jens Katzer & Peter Langendörfer (2020). Metal Fillers as Potential Low Cost Countermeasure against Optical Fault Injection Attacks. In *2020 IEEE East-West Design Test Symposium (EWDTS)*, 1–6.

[4] Dmytro Petryk, Zoya Dyka & Peter Langendörfer (2020). Sensitivity of Standard Library Cells to Optical Fault Injection Attacks in IHP 250 nm Technology. In *2020 9th Mediterranean Conference on Embedded Computing (MECO)*, 1–4.

[5] Dmytro Petryk, Zoya Dyka, Roland Sorge, Jan Schäffner & Peter Langendörfer (2021). Optical Fault Injection Attacks against Radiation-Hard Shift Registers. In *2021 24th Euromicro Conference on Digital System Design (DSD)*, 371–375.

[6] IHP BiCMOS technology (2022). URL `https://www.ihpmicroelectronics.com/en/services/mpw-prototyping/sigec-bicmostechnologies.html`.