Back-side Laser Fault Injection Attacks against Radiation-Hardened Shift-Registers

R. Hegewald[1,2], J. Schäffner[2], Z. Dyka[2,3], I. Kabin[2], M. Krstic[1,2], and D. Petryk[2]

[1]University of Potsdam, Potsdam, Germany
[2]IHP – Leibniz Institute for High Performance Microelectronics, Frankfurt (Oder), Germany
[3]BTU Cottbus-Senftenberg, Cottbus, Germany

38th Crypto Day, 6/7 March 2025

Semiconductor devices utilizing cryptographic ciphers must be resistant against physical attacks. One class of physical attacks – known as fault injections (FIs) – aims to manipulate stored/processed data while the device executes an operation with a secret/private key. Successful manipulation, e.g. changing the output of single logic cells, can cause a leakage of secret data or allow to extract it through fault analysis. One method of FI attacks exploits the sensitivity of semiconductor devices to light. These attacks are implemented using a LASER.

The most frequently attacked block of cryptographic devices is memory, e.g. registers. A common method of improving resistance against FI attacks is to apply redundancy. Radiation hardened designs developed for space application are proven to be less susceptible to short electromagnetic waves compared to standard designs. Thus, they seem to be an attractive option for improving resistance against physical attacks. Junction Isolated Common Gate (JICG) is one of the radiation-hardening techniques that is based on transistor redundancy [4]. In the past, JICG shift registers were successfully manipulated through the front-side of a chip [3]. However, metal fillers placed on top of the transistors decrease the effectiveness of such attacks [2]. In this work, we conducted optical FI attacks against JICG shift registers through the back-side and assessed the influence of substrate thickness on the success of these attacks.

We experimented with JICG registers manufactured in IHP 250 nm technology [1]. The chips were bonded as flip-chips on a PCB exposing the chip's substrate. To assess the influence of substrate thickness on the success of the attacks, we used chips with different thicknesses: 30 µm, 50 µm, 100 µm, 150 µm and 750 µm. Attacks were performed using an FI setup with a Riscure 1064 nm near-infrared laser. To successfully change the logic state of a single flip-flop, both redundant transistors of the flip-flop must be illuminated simultaneously with the laser beam. Hence, the attacks were performed using 5x and 20x magnification objectives to achieve a relatively big laser beam spot. In our attack,

crypto day matters 38 (2025)
Beiträge vom 38. Kryptotag, 06.-07. März 2025, Hamburg.
doi:10.18420/cdm-2025-38-13

we varied the laser beam power while applying a constant pulse duration of 150 ns. Table 1 shows the results of the performed fault injection experiments.

Thickness	**Objective**	**Type of Fault**	**Power**
30 µm	5x	Set	28%
		Reset	29%
	20x	Set	9%
		Reset	10%
50 µm	5x	Set	28%
		Reset	28%
	20x	Set	12%
		Reset	12%
100 µm	5x	Set	32%
		Reset	32%
	20x	Set	13%
		Reset	14%
150 µm	5x	Set	32%
		Reset	33%
	20x	Set	18%
		Reset	17%

Table 1: Measurements for Fault Types and Different Thicknesses

We were able to inject transient repeatable bit-set ($0 \rightarrow 1$) and bit-reset ($1 \rightarrow 0$) faults in all chips, except for the one with 750 µm thick substrate. As expected, increased substrate thickness requires higher laser beam output power to successfully inject a fault.

References

[1] IHP (2025). IHP : Leibniz Institute for High Performance Microelectronics. `https://www.ihp-microelectronics.com/`. [Accessed 13-02-2025].

[2] 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.

[3] Dmytro Petryk, Zoya Dyka, Roland Sorge, Jan Schaffner & Peter Langendorfer (2021). Optical Fault Injection Attacks against Radiation-Hard Shift Registers. In *2021 24th Euromicro Conference on Digital System Design (DSD)*, 371–375. IEEE. URL `http://dx.doi.org/10.1109/DSD53832.2021.00062`.

[4] R. Sorge, J. Schmidt, Ch. Wipf, F. Reimer, F. Teply & F. Korndörfer (2021). JICG CMOS transistors for reduction of total ionizing dose and single event effects in a 130 nm bulk SiGe BiCMOS technology. *Nuclear Instruments and Methods in Physics Research Section A: Accelerators, Spectrometers, Detectors and Associated Equipment* **987**, 164 832. ISSN 0168-9002. URL `https://www.sciencedirect.com/science/article/pii/S0168900220312298`.