Laser Fault Injection Attacks against IHP Chips

Dmytro Petryk[1] Zoya Dyka[1] Peter Langendörfer[1,2]

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

[2]BTU Cottbus-Senftenberg
Cottbus, Germany

32nd Crypto Day, 15 January 2021

Nowadays semiconductor devices are subject to various types of physical attacks, e.g. fault injection (FI) attacks. The goal of FI is to get access to sensitive data stored in a secure device by injecting fault(s) via an external source. In this work we present our successful laser FI attacks against different chips Libval013 implemented in IHP's 130 nm as well as Livbal025 and IHP Resistive Random Access Memory (RRAM) in IHP's 250 nm technology. TABLE 1 describes chips successfully attacked in our experiments. We performed laser FI attacks using a Riscure Diode Laser Station [1] with a multi-mode red (808 nm) laser source. Hence, all attacks were performed through the front-side of the chip. We chose red laser due to the ease of the preparation process of the selected chips for front-side FI attacks compared to the preparation process for rear-side attacks.

Table 1: Description of successfully attacked chips in our experiments

Chip	Libval025	Libval013	RRAM
Manufacturing technology	250 nm (old)	130 nm (recent)	250 nm (recent)
Number of metal layers	5	7	5
IHP library	standard		
Metal fillers	no	yes	
Gate/cell	INV, NOR, NAND, FF		1 Transistor - 1 Resistor
Mode of attack	in operation		standalone
Observable transitions	INV, NOR, NAND: 1→0; FF: 0→1		[1]0↔1; 0↔US; US↔1; 0↔Stuck-at 1; 1↔Stuck-at 1; US↔Stuck-at 1

Recent manufacturing technologies use metal fillers – small metal structures placed in different metal layers – to maintain mechanical stiffness of the chips, e.g. in IHP technologies [2]. They are obstacles for laser beams. Thus, we

[1] due to the specific of RRAM it has 4 defined states [3], where US is undefined state.

crypto day matters 32 (2021)
Beiträge vom 32. Kryptotag, 15.01.2021, online.
doi:10.18420/cdm-2021-32-22

expected that metal fillers decrease the success rate of laser FI attacks and can be used as a low-cost countermeasure against optical inspection and FI attacks. To evaluate this we attacked IHP chips manufactured with and without metal fillers, see TABLE 1. Our results show that logic gates (invertors, NOR, NAND and flip-flops) in chips manufactured without metal fillers are more sensitive to FI attacks than the logic gates in chips with metal fillers. When attacking IHP RRAM we were able to influence RRAM cells that are covered as well as not covered by metal fillers with a similar success rate [3]. As it is well known that RRAM cells are sensitive to heat, we assume that in case of the RRAM cells the metal fillers are local heating sources for the Metal Insulator Metal structures due to the laser illumination and by that the reason of our successful FI. To clarify this assumption further investigations are required.

Acknowledgement

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.

References

[1] Riscure (2011). *Diode Laser Station. Inspector Datasheet.* URL `https://www.riscure.com/security-tools/inspector-hardware/`.

[2] IHP BiCMOS technology (2020). URL `https://www.ihpmicroelectronics.com/en/services/mpw-prototyping/sigec-bicmostechnologies.html`.

[3] D. Petryk, Z. Dyka, E. Perez, I. Kabin, J. Katzer, J. Schäffner & P. Langendörfer (submitted). Sensitivity of HfO_2-based RRAM Cells to Laser Irradiation. *Microprocessors and Microsystems* .