

Hardware Moving Target Defenses against Post-Silicon Side-Channel Leakages

Saleh Khalaj Monfared
Worcester Polytechnic Institute
Worcester, MA, USA
Email: skmonfared@wpi.edu

Kyle Mitard
Worcester Polytechnic Institute
Worcester, MA, USA
Email: kmitard@wpi.edu

Domenic Forte
University of Florida
Gainseville, FL, USA
Email: dforte@ece.ufl.edu

Shahin Tajik
Worcester Polytechnic Institute
Worcester, MA, USA
Email: stjajik@wpi.edu

Abstract—Pre-silicon tools for hardening hardware against side-channel and fault injection attacks have become popular recently. However, the security of the system is still threatened by sophisticated physical attacks, which exploit the physical layer characteristics of the computing system beyond the integrated circuits (ICs) and, therefore, bypass the conventional countermeasures. Further, environmental conditions for the hardware can also impact side-channel leakage and fault vulnerability in unexpected ways that are challenging to model in pre-silicon. Thus, attacks cannot be addressed solely by conventional countermeasures at higher layers of the compute stack due to the lack of awareness about the events occurring at the physical layer during runtime. In this paper, we first discuss why the current pre-silicon security and verification tools might fail to achieve security against physical threats in the post-silicon phase. Afterward, we provide insights from the fields of power/signal integrity (PI/SI), and failure analysis (FA) to understand the fundamental issue with the failed current practices. We argue that hardware-based moving target defenses (MTDs) to randomize the physical fabric’s characteristics of the system can mitigate such unaccounted post-silicon threats. We show the effectiveness of such an approach by presenting the results of two case studies in which we perform powerful attacks, such as impedance analysis and laser voltage probing. Finally, we review the overhead of our proposed approach and show that the imposed overhead by MTD solutions can be addressed by making them active only when a threat is detected.

I. INTRODUCTION

The threats to the physical security of computer chips and countermeasures have been widely researched. However, with the rise of more modular and complex computing systems, the physical security of the system is threatened by more sophisticated physical attacks. Pre-silicon tools for assessing a device’s vulnerability to side-channel and fault injection attacks have gained traction recently. This approach uses leakage and fault emulators to analyze the device’s model rather than measuring actual physical leakage after fabrication. The goal is to automate the vulnerability detection process earlier in development, reducing the overall security risk.

However, it has been repeatedly shown that after the die packaging and the integration of the chip to a printed circuit board (PCB), information leakage and fault vulnerability could still exist at the system level in certain conditions [1]. Moreover, such pre-silicon defenses are ineffective against novel physical side-channels and fault injection attacks based on

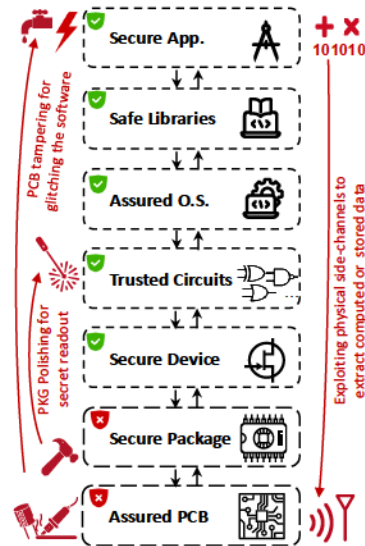


Fig. 1: Abstraction layers of edge computing devices and potential threats.

techniques used in power/signal integrity (PI/SI) [2], electromagnetic compatibility/interference (EMC/EMI) [3], failure analysis (FA) [4], and electrostatic discharge (ESD) [5]. Further, environmental conditions experienced by the hardware can also impact leakage and fault sensitivity in unexpected ways that are challenging to model pre-silicon [1].

The primary reason for the failure of these tools is the unforeseen impact of the “analog” features at the physical layer of the system. These threats cannot be addressed solely by conventional security mechanisms at higher layers (see Fig. 1) of the compute stack (e.g., secure protocols or algorithmic side-channel/fault countermeasures) due to the lack of awareness about the events occurring at the physical layer of a computing machine. Hence, holistic and scalable tamper detection techniques, sensors for physical integrity monitoring beyond chips, and novel response mechanisms at the physical level are required to create a security foundation for the upper abstraction layers of the computing machine. Hence, in this work, we ask the following research questions: *Is it possible to deploy sensors to detect physical attack attempts, dial in post-*

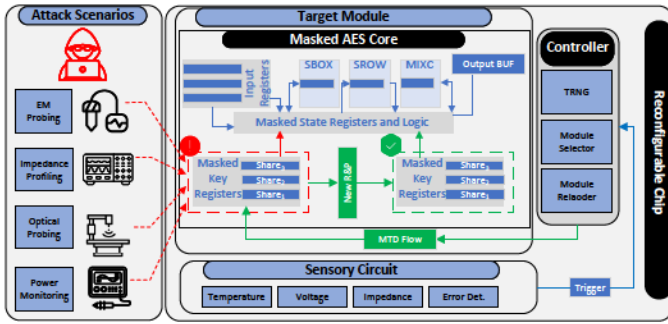


Fig. 2: High-level overview of hardware Moving Target Defense (MTD)

silicon countermeasures, and continue the operation without interruption without imposing a large size, weight, and power (SWaP) overhead?

Contribution. In this work, we answer the above question positively. We first discuss why the current pre-silicon security and verification tools fail to provide holistic security against physical threats in the field. Afterward, we will provide insights from other fields, e.g., electromagnetic compatibility (EMC) and failure analysis (FA), to understand the fundamental issue with the failed current practices. We argue why we should focus more on detecting and responding to physical attacks during runtime. We present detection methods to detect physical attack attempts on the system. Upon detection of the attack, we propose real-time hardware-based moving target defenses (MTD) using reconfigurable technologies to randomize the placement and routing of the design to avert the attacks. Finally, we discuss the countermeasure overhead.

II. BACKGROUND

A. Post-Silicon Threats

1) *Insights from EMC and PI/SI:* Any electronic device generates some amount of electromagnetic radiation. We consider electronics as closed systems, but, the current flowing through circuits and wires is never fully contained. This energy can be propagated through the air as *radiated emissions* and conducted along (or coupled onto) interconnecting I/O or power cables, which is referred to as *conductive emissions*. Such a system as a whole behaves like an antenna, and a chip's die is only a single component of this complex system. While mitigating the electromagnetic leakage at the RTL, netlist, or even layout level of a chip is necessary, it is not sufficient if we do not consider the effect of the package and PCB's power delivery network (PDN) as well as other signal traces on the system on the radiation behavior. By packaging the chip, soldering it to a PCB, or even connecting a cable to the PCB in the field, the entire physical characteristics of the system, e.g., impedance, coupling, etc., change as well as its radiation and reception behavior. On the other hand, backscattered impedance measurement methods from the field of power/signal integrity (PI/SI) can be deployed to probe the tiniest impedance variations caused by the data on the chip.

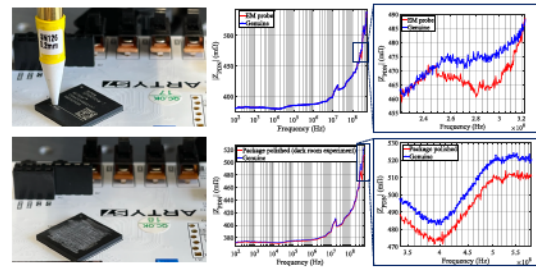


Fig. 3: Examples of tamper events on the system and their detection using the on-FPGA VNA [9].

2) *Insights from FA:* FA tools are essential to debug millions to billions of transistors on a chip after manufacturing. The IC debug techniques deploy laser or electron beams to interact with single transistors. Naturally, the resolution of FA tools must keep up with the trend of transistor miniaturization to resolve single transistors. However, these tools can also be utilized to probe transistors and extract secret information from the chip. Hence, there is no place to hide on the chip if the IC debug tools can resolve every single transistor on the die.

3) *Impact of Environmental Conditions:* IC behavior is known to change over time due to temperature and aging. Thermal effects can slow the movement of the electrons through interconnects, cause electromigration that shortens the lifespan of a chip, and impact logic gate rise and fall times [6]. More recently, it has been observed that heat can be used as a covert channel, which makes it easier to inject faults and glitches. Even correct implementations of masking schemes exhibit unexpected power leakage [1]. Silicon aging varies across a chip and increases susceptibility to collision timing attacks [7] and de-obfuscation [8].

B. Post-Silicon Solutions

To analyze the system's side-channel leakage and fault vulnerability, one should simulate the analog behavior of the system in various conditions in different domains. Such simulations are complex and time-consuming and, thus, are not common in practice. Due to the complexity of simulating the entire system's side-channel leakages and fault vulnerabilities in an ever-changing adversarial environment and the vulnerability of the system to sophisticated attacks based on PI, EMC, and FA methods, we should shift our attention from the prevention of the threats to detecting and responding to them during the runtime.

1) *Attack Detection:* Attack detection is one of the under-researched areas in hardware security. Detecting the threats even before the occurrence of the attack should be the goal of designing sensors and detection mechanisms. Some classes of physical attacks require physical access and modifications to the system. Examples of those modifications include connecting a cable, removing the heatsink, or replacing components. By detecting such tamper events, we can detect the attack attempt before the attack itself [9]. For attacks without tampering requirements, we advocate for deploying various sensors at

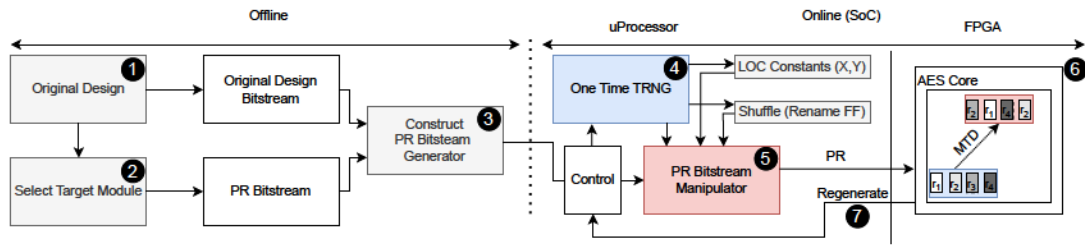


Fig. 4: High-level block-diagram description of hardware MTD using real-time partial reconfiguration [10]

the die level, a practical and effective strategy to monitor the environment for malicious changes in temperature and voltage. Such sensors can also be used to track chip aging.

2) *Attack Response*: Another less explored area in hardware security is the response to an attack. In other words, it is unclear what the right approach would be after detecting an attack. The prevailing assumption is that the memories containing secret information can be zeroized upon the detection of an attack. However, in many real-world scenarios, the system should continue its operation, and the mission should succeed regardless of the attack. In such scenarios, similar to the cyber domain, MTD strategies can be adopted to mitigate unknown vulnerabilities [11]. Naturally, MTD schemes impose a high power, performance, area (PPA) overhead to the system, which might not be appropriate for applications with low size, weight, and power (SWaP) requirements. Hence, adaptive MTD-based countermeasures should be activated once a threat is detected. Moreover, various defenses can be dialed in depending on the threat level.

III. IMPEDANCE AND VOLTAGE SENSORS

A. Impedance Sensors

Depending on the physical attack's requirements, adversaries might need to (i) place probes in the proximity of the IC packages, (ii) create physical connections between their probes and the PCB, or (iii) physically tamper with the PCB's components, chip's package, or substitute the entire PCB to prepare the device for the attack. While tamper-proof enclosures prevent and detect physical access to the system, their high manufacturing cost and incompatibility with legacy systems make them unattractive for many low-cost scenarios. A lightweight solution is an on-die network analyzer, which can sense the impedance variations of the system's power delivery network (PDN) and detect various classes of tamper events. Without any modifications to the system, such embedded network analyzers can be deployed on FPGAs to extract the frequency response of the PDN. The analysis of these frequency responses reveals different classes of tamper events from board to chip level. Such a wideband impedance characterization could surprisingly reveal very sophisticated tampering and modifications to the system, e.g., (i) the addition/removal of PCB components, (ii) the connection of a probe/wires to the PCB, (iii) the presence of an EM probe close to the IC package, (iv) and modifications to the IC package, see Fig. 3.

B. Delay-based Sensors

One similarity among different active physical attacks is their instant disturbance on a set of physical parameters, e.g., temperature and current. The local temperature and current variations can affect the propagation delays of the electrical signals in the delay-dependent circuits, such as ring oscillators (ROs) and time-to-digital converters (TDCs). Deploying delay-based sensors is the primary way for sensing analog disturbances on the chip PDN caused by voltage glitches [12], EM glitches [13], and laser irradiation [14].

IV. HARDWARE MOVING TARGET DEFENSE VIA RECONFIGURABILITY

Partial Reconfiguration (PR) is a feature of mainstream field programmable gate arrays (FPGAs), allowing for dynamic modifications of a portion of the FPGA circuit without needing a complete system reboot. At the same time, the rest of the system continues to operate uninterrupted, [15]. The use of PR in FPGAs is particularly advantageous in mission-critical applications where system downtime is not acceptable. Several side-channel countermeasures [16], [17], [18], [19], [20], [21] deploy PR to defeat power and electromagnetic (EM) analysis attacks. These efforts merely utilize PR to introduce jitter (realized by delay) to defeat power side channels. Other approaches include relocation of the functions to defeat EM attacks. The main drawback here is the limited available number of randomized PRs, leading to a linear increase in the complexity of the attack. Moreover, the partial bitstreams in these schemes have to be stored on external non-volatile memory and invoked during runtime, resulting in a very high overhead.

Generally, FPGA IDEs present significant limitations, including a slow performance for real-time applications and a lack of bitstream relocation support, constraining the reconfigurability [22]. Several notable tools have emerged to address these challenges. For instance, the open-source tool Byte-man [22] has substantially improved bitstream manipulation capabilities for AMD/Xilinx FPGAs. It enhances efficiency, speed, and compatibility by supporting the merging of clock, Configurable Logic Block (CLB), and Block RAM data, along with implementing different merge strategies. These bitstream manipulation tools are crucial, as they provide the ability to generate and deploy partial bitstreams in real-time.

The framework is divided into offline and online procedures. The offline part is executed once for a given target. This target

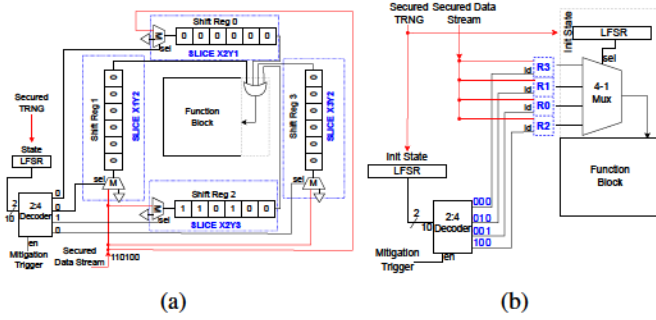


Fig. 5: Real-time (a) Target Slice Multiplexer and (b) Register Sequence Multiplexer.

could be any IP core (e.g., AES encryption core) containing sensitive information that should be protected. Using a high-level scripting language (specifically TCL), the user indicates targeted modules. Multiple partial bitstreams, as well as the original bit file, are generated at this stage. The constraints, including the possible range for slices, regional locations, and range possible of FFs [23] in reconfiguration, are identified. In the online phase, a lightweight Operating System (OS) (such as Ubuntu) is utilized in the SoC to generate and control the reconfiguration. A secured one-time pseudo-random number generator (PRNG) [24] is deployed, and the randomness is passed to the PR-generator unit each time. The PR-generator unit incorporates a bitstream manipulator (Byteman[22] in our case) with pre-defined constraints. In this step, randomized LOC (the placement assignment of a logic cell in AMD FPGAs) and shuffling constraints are selected, and the correspondent partial reconfiguration bitstream is generated based on the existing original bitstream. Upon generating the PR, the FPGA is programmed as the trigger signal is received.

It is possible to have multiple instances of the same target circuit in distinct slices and choose one randomly to be connected periodically. The obvious trade-off here is the area overhead caused by all those additional blocks. However, as a simple mitigation, a real-time target slice multiplexer (see Fig. 5a) could be considered. Another approach is to deploy a fine-grained MTD which involves hardware scrambling of register references. Fig. 5b illustrates a simple digital design diagram of a real-time register sequence multiplexer. This yields to randomization of the data order every time the target registers are loaded. The vital part of this mitigation is maintaining the initial state so that the function block can read the data in the correct format. Theoretically, this method realizes the upper bound of super-exponential ($\mathcal{O}(n!)$) complexity against trial-based attacks.

V. CASE STUDIES

We assess the effectiveness of the proposed approach against powerful *backscattered* side-channel attacks. In such attacks, the attacker stimulates the target device in various forms, e.g., microwave radiations [2], [3], [25], near-infrared laser beams [26], [4], or even electron beams [27] and measures the reflected signals from it. The reflected signals are modulated

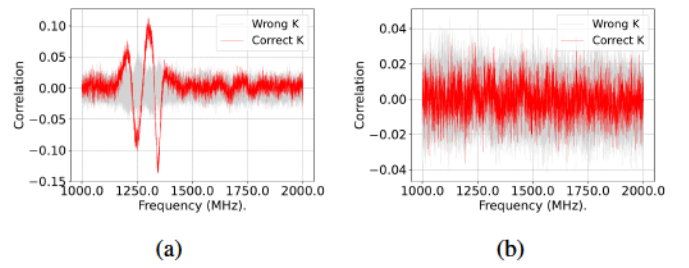


Fig. 6: Frequency profile of impedance attack for $N = 10,000$ traces on the first byte key: (a) without MTD (b) with MTD.

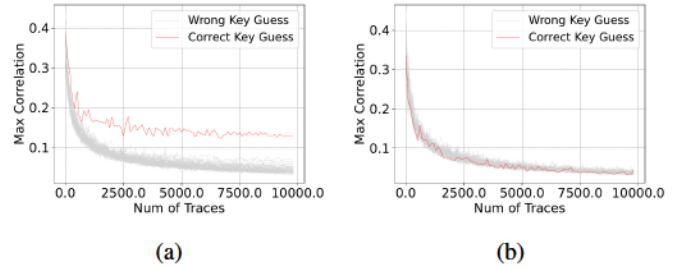


Fig. 7: Impedance leakage with respect to the number of traces on the first-byte key: (a) without MTD (b) with MTD.

depending on the state of a circuit or memory contents and, thus, can be exploited by the attacker to recover secrets from the chip. Among these backscattered methods, non-invasive stimulation using microwave signals through the system's power delivery network (PDN) [2], [25] and laser beams through silicon backside [26], [4] are the most threatening one due to their effectiveness. The main reason behind the modulation of the reflected signal is the data-dependent changes in the impedance of the circuit and the absorption/refractive coefficient of the silicon. In contrast to most of the conventional side-channel attacks (e.g., power and EM analysis), impedance analysis and laser voltage probing attacks *enable the extraction of static data*.

A. Impedance Analysis Attack

We follow the same procedure described in [2] to perform a correlation impedance attack on a target FPGA. For this aim, we carry out two sets of correlation analyses on a single byte of the Key in an AES-128 encryption implementation. First, we execute the attack on unprotected AES implementation to extract the key and identify the number of impedance profiles to guess the correct key. Then, we enable reconfiguration-based MTD and perform a similar attack. In this experiment, we set our defensive MTD to conduct the reconfiguration for every $PRRate = 16$ AES encryption.

We employed a Keysight ENA Network Analyzer E5080A, for scattering impedance measurements. We utilized a NewAE CW305 board [28], equipped with a 28 nm AMD/Xilinx Artix-7 FPGA (XC7A100T), as it allows direct access to the FPGA's core (V_{CCINT}) PDN. Fig. 7 shows the frequency-dependent impedance correlation leakage of the first byte of the AES

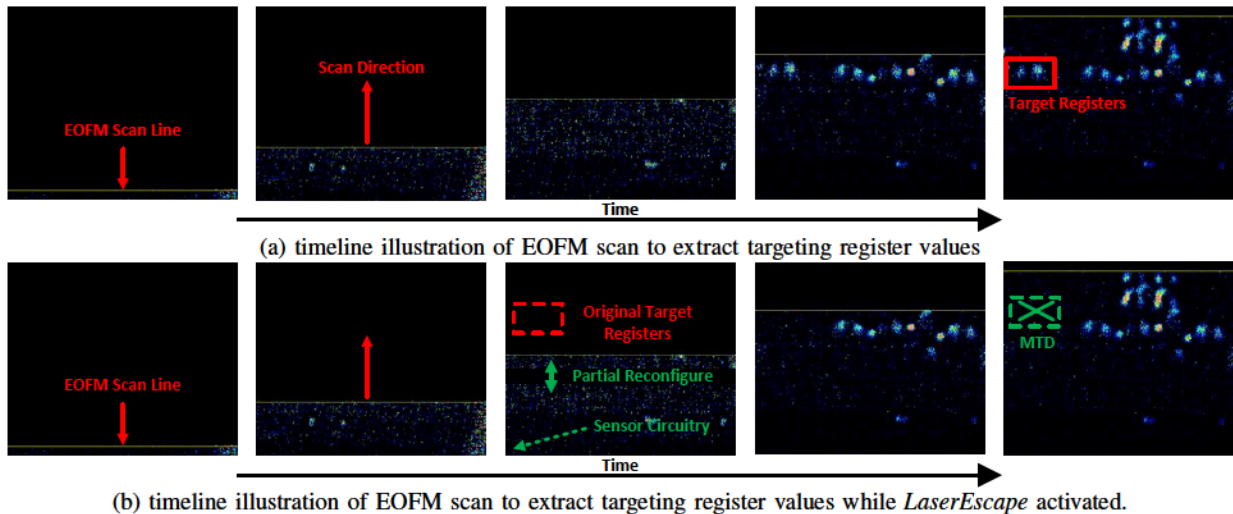


Fig. 8: EOFM probing attack timeline on images captured during laser scanning from the backside of the FPGA.

key for $N = 10,000$ traces. As highlighted in Fig. 6b, the maximum correlation leakage decreases as MTD mitigation is deployed. Furthermore, we conduct a trace-based leakage study by carefully analyzing the correlation leakage in terms of the traces captured from the device. Fig. 7 depicts the correlation analysis for our case studies. As shown in Fig. 7a, an unprotected AES key byte can be extracted by utilizing a couple of thousands of traces. On the other hand, if the reconfiguration mitigation is activated, as illustrated in Fig. 7b, the correlation leakage decreases significantly to the point that 10,000 traces are not enough for the analysis to successfully guess the correct key byte.

B. Laser Voltage Probing/Imaging Attack

In Laser Voltage Imaging (LVI) or Electro-Optical probing/Frequency Modulation (EOFM) attacks, the adversary can locate the target registers and their contents (specifically cryptographic keys) using high-end laser microscopy by forcing the target registers to switch in a specific frequency. We utilized a Hamamatsu PHEMOS-X FA microscope with a $1.3 \mu\text{m}$ laser source and objective lenses of 5X/0.14NA, 20X/0.6NA, 50X/0.76NA, and 71X to zoom into the target elements. For the EOFM process, the target device is scanned by a laser using galvanometric mirrors. Moreover, our Device Under Test (DUT) for this experiment was a Digilent’s Genesys 2 development board, equipped with a Kintex-7 FPGA from Xilinx/AMD (part number XC7K325T-2FFG900C).

Similar to [29], a profiling attack is mounted on key registers implemented using flip-flops and synchronous reset. The localization attack is achieved by switching the *reset* signal of the DUT[29]. Figure8a illustrates the timeline of an EOFM scan focused on a target area. As shown, the target registers are precisely localized at the selected frequency (i.e., the *reset* frequency) once the EOFM scanner line aligns with the area. To evaluate our approach, we conducted a similar EOFM attack in the presence of the proposed MTD countermeasure. A group of eight FDRE registers assumed to

hold a cryptographic algorithm’s master key (e.g., AES) was selected as the target. Figure8b depicts the timeline of the EOFM scan aimed at these FDRE registers. Unlike the attack shown in Fig. 8a, when the scanning laser approaches the physical locations of the target FDREs, the MTD is triggered, and PR is executed in real-time to move the target circuitry out of the field of view of the lens.

C. Overhead Analysis

For delay overhead, the offline part of the MTD process is not considered, as it is executed only once during the design. The online part comprises a real-time randomized PR generation off-FPGA in the SoC’s processor, which incurs a constant delay for each bitstream generation. The bitstream loading is handled via ICAP interface. For our evaluations on ARM/FPGA Zynq-7000 SoC, ICAP operates at 100MHz with a 400MB/s data transfer rate, resulting the PR loading to take approximately 74 clock cycles for each CLB [30].

We assume that the PR is performed on-demand and is triggered externally. As an example, we consider an AES implementation in our evaluations. Without using MTD, this particular implementation utilizes 7426 LUTs and 3581 FFs on the DUT. Area overhead for the register shuffling method (used against impedance attack) is negligible ($< 0.1\%$) since it is executed within the same Reconfigurable Module. In the case of coarse grain randomization (used as the mitigation against laser attack), the overhead [31] in AES circuits will be up to 14% in terms of number of LUTs and FFs.

Table I details the delay and area overhead of our MTD method for the AES implementation under different reconfiguration frequencies and number of reconfiguration modules.

VI. CONCLUSION

This paper reviewed the post-silicon threats to an already hardened hardware. We discussed how the unforeseen impact of analog features at the physical layer of the system in

TABLE I: Delay/Area overhead in different configurations.

Delay Overhead			
PR Gen Freq	2	8	16
Average Overhead (us)	446	118	63

Area Overhead			
RM Number	2	4	8
CLB Overhead (%)	9.4	12.1	14.8

different environments can create side-channel leakages. Based on these threats, we proposed hardware-based moving target defense (MTD) approaches to deal with such unaccounted leakages. We demonstrated that hardware-based MTD can be realized through either the PR feature of conventional FPGAs or multiplexers on ASICs to randomize the placement and routing of sensitive circuits. We used open-source bitstream manipulator tools to build a real-time PR-based countermeasure for programmable SoCs/FPGAs. By presenting two case studies, we showed the effectiveness of the MTD schemes. Finally, we examined the overhead of our proposed scheme in terms of delay and resource utilization.

ACKNOWLEDGMENT

This effort was sponsored by NSF Grants CNS-2150123, CNS-2150122, CNS-2338069, and Draper scholarship.

REFERENCES

- [1] D. M. Mehta, M. Hashemi, D. S. Koblach, D. Forte, and F. Ganji, "Bake it till you make it: Heat-induced power leakage from masked neural networks," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2024.
- [2] S. K. Monfared, T. Mosavirik, and S. Tajik, "Leakyohm: Secret bits extraction using impedance analysis," *Cryptology ePrint Archive*, 2023.
- [3] S. Kaji, D. Fujimoto, M. Kinugawa, and Y. Hayashi, "Echo tempest: Em information leakage induced by iemi for electronic devices," *IEEE Transactions on Electromagnetic Compatibility*, 2023.
- [4] T. Krachenfels, F. Ganji, A. Moradi, S. Tajik, and J.-P. Seifert, "Real-world snapshots vs. theory: Questioning the t-probing security model," in *2021 IEEE symposium on security and privacy (SP)*. IEEE, 2021, pp. 1955–1971.
- [5] J. Loughry and K. Rasmussen, "Basilisk: Remote code execution by laser excitation of {P-N} junctions without insider assistance," in *18th USENIX WOOT Conference on Offensive Technologies (WOOT 24)*, 2024, pp. 245–261.
- [6] J. Keane and C. H. Kim, "Transistor aging," *IEEE Spectrum*, vol. 48, no. 5, pp. 28–33, 2011.
- [7] M. Ebrahimabadi, B. Fadaeinia, A. Moradi, and N. Karimi, "Does aging matter? the curious case of fault sensitivity analysis," in *2022 23rd International Symposium on Quality Electronic Design (ISQED)*. IEEE, 2022, pp. 84–89.
- [8] Z. Guo, S. Chowdhury, M. M. Tehranipoor, and D. Forte, "Permutation network de-obfuscation: A delay-based attack and countermeasure investigation," *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, vol. 16, no. 2, pp. 1–25, 2020.
- [9] T. Mosavirik, P. Schaumont, and S. Tajik, "Impedanceverif: On-chip impedance sensing for system-level tampering detection," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 301–325, 2023.
- [10] S. K. Monfared, D. Forte, and S. Tajik, "Randohm: Mitigating impedance side-channel attacks using randomized circuit configurations," *arXiv preprint arXiv:2401.08925*, 2024.
- [11] D. S. Koblach, F. Ganji, D. Forte, and S. Tajik, "Hardware moving target defenses against physical attacks: Design challenges and opportunities," in *Proceedings of the 9th ACM Workshop on Moving Target Defense*, 2022, pp. 25–36.
- [12] S. Moini, D. Kansagara, D. Holcomb, and R. Tessier, "Fault recovery from multi-tenant fpga voltage attacks," in *Proceedings of the Great Lakes Symposium on VLSI 2023*, 2023, pp. 557–562.

- [13] M. Paquette, B. Marquis, R. Bainbridge, and J. Chapman, "Visualizing electromagnetic fault injection with timing sensors," in *2021 IEEE Physical Assurance and Inspection of Electronics (PAINE)*. IEEE, 2021, pp. 1–8.
- [14] S. K. Monfared, K. Mitard, A. Cannon, D. Forte, and S. Tajik, "Lasereescape: Detecting and mitigating optical probing attacks," *arXiv preprint arXiv:2405.03632*, 2024.
- [15] D. Koch, J. Torresen, C. Beckhoff, D. Ziener, C. Dendl, V. Breuer, J. Teich, M. Feilen, and W. Stechele, "Partial reconfiguration on fpgas in practice—tools and applications," in *ARCS 2012*. IEEE, 2012, pp. 1–12.
- [16] N. Mentens, B. Gierlichs, and I. Verbauwhede, "Power and fault analysis resistance in hardware through dynamic reconfiguration," in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2008, pp. 346–362.
- [17] T. Güneysu and A. Moradi, "Generic side-channel countermeasures for reconfigurable devices," in *International workshop on cryptographic hardware and embedded systems*. Springer, 2011, pp. 33–48.
- [18] J. Heyszl, S. Mangard, B. Heinz, F. Stumpf, and G. Sigl, "Localized electromagnetic analysis of cryptographic implementations," in *Topics in Cryptology—CT-RSA 2012: The Cryptographers' Track at the RSA Conference 2012, San Francisco, CA, USA, February 27–March 2, 2012. Proceedings*. Springer, 2012, pp. 231–244.
- [19] B. Hettwer, J. Petersen, S. Gehrler, H. Neumann, and T. Güneysu, "Securing cryptographic circuits by exploiting implementation diversity and partial reconfiguration on fpgas," in *2019 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE, 2019, pp. 260–263.
- [20] I. Bow, N. Bete, F. Saqib, W. Che, C. Patel, R. Robucci, C. Chan, and J. Plusquellic, "Side-channel power resistance for encryption algorithms using implementation diversity," *Cryptology*, vol. 4, no. 2, p. 13, 2020.
- [21] N. Khan, B. Hettwer, and J. Becker, "Moving target and implementation diversity based countermeasures against side-channel attacks," in *International Symposium on Applied Reconfigurable Computing*. Springer, 2021, pp. 188–202.
- [22] K. Manev, J. Powell, K. Matas, and D. Koch, "byteman: A bitstream manipulation framework," in *2022 International Conference on Field-Programmable Technology (ICFPT)*. IEEE, 2022, pp. 1–9.
- [23] Xilinx. (2023, May) Xilinx constraints guide. [Online]. Available: <https://www.xilinx.com/xilinx-14/cgd.pdf>
- [24] K. H. Tsoi, K. H. Leung, and P. H. W. Leong, "Compact fpga-based true and pseudo random number generators," in *11th Annual IEEE Symposium on Field-Programmable Custom Computing Machines, 2003. FCCM 2003*. IEEE, 2003, pp. 51–61.
- [25] M. S. Awal and M. T. Rahman, "Disassembling software instruction types through impedance side-channel analysis," in *2023 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. IEEE, 2023, pp. 227–237.
- [26] S. Tajik, H. Lohrke, J.-P. Seifert, and C. Boit, "On the power of optical contactless probing: Attacking bitstream encryption of fpgas," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 2017, pp. 1661–1674.
- [27] E. Amini, T. Kiyani, L. Renkes, T. Krachenfels, C. Boit, J.-P. Seifert, J. Jatzkowski, F. Altmann, S. Brand, and S. Tajik, "Electrons vs. photons: Assessment of circuit's activity requirements for e-beam and optical probing attacks," in *ISTFA 2023*. ASM International, 2023, pp. 339–345.
- [28] NewAE. (2023, May) Cw305 artix fpga target. [Online]. Available: <https://rtfm.newae.com/Targets/CW30520Artix20FPGA>
- [29] H. Lohrke, S. Tajik, C. Boit, and J.-P. Seifert, "No place to hide: Contactless probing of secret data on fpgas," in *Cryptographic Hardware and Embedded Systems—CHES 2016: 18th International Conference, Santa Barbara, CA, USA, August 17–19, 2016, Proceedings 18*. Springer, 2016, pp. 147–167.
- [30] Q. Tang, Z. Wang, B. Guo, L.-H. Zhu, and J.-B. Wei, "Partitioning and scheduling with module merging on dynamic partial reconfigurable fpgas," *ACM Transactions on Reconfigurable Technology and Systems (TRET)*, vol. 13, no. 3, pp. 1–24, 2020.
- [31] M. M. Ahmadi, L. Alrahis, O. Sinanoglu, and M. Shafique, "Fpga-patch: Mitigating remote side-channel attacks on fpgas using dynamic patch generation," in *2023 IEEE/ACM International Symposium on Low Power Electronics and Design (ISLPED)*. IEEE, 2023, pp. 1–6.