On Optical Attacks Making Logic Obfuscation Fragile

Leonidas Lavdas, M Tanjidur Rahman, Mark Tehranipoor, and Navid Asadizanjani
Florida Institute for Cybersecurity (FICS) Research, Department of Electrical & Computer Engineering,
University of Florida, Gainesville, 32611, FL, USA.
Email: leonidas.lavdas@ufl.edu, mir.rahman@ufl.edu, nasadi@ece.ufl.edu

***Abstract*—**
The backside of modern Integrated Circuits (ICs) is becoming an open backdoor for malicious hardware attackers to take advantage of. Aided by new Failure Analysis (FA) optical techniques, e.g., Photon Emission Analysis (PEA), optical probing, and Laser Fault Injection (LFI), hackers pose a serious threat to the confidentiality, integrity and availability of sensitive information on a chip. In addition, optical backside attacks can risk semiconductor intellectual property (IP) protection mechanisms, such as logic locking. In this work, we review some of these failure analysis techniques through the lens of Optical Attack. We also review combinational and sequential Logic Locking, and then focus on corresponding state space obfuscation methodology. Attack procedures are then described on how to break into these obfuscation systems, and finally, existing countermeasures and their limitations are discussed.

I. INTRODUCTION

Microelectronics Failure Analysis (FA) has experienced a paradigm shift in the past two decades due to interconnects implemented with ten or more layers. The Silicon Debugging and Diagnosis (SDD) techniques used for defect localization in functional circuit can no longer interact with the active device layers directly. Therefore, FA methods from chip backside are invented to match with faster yield analysis and aggressive time-to-market requirements. Besides, new packaging techniques like flip-chip, with exposed bulk silicon (i.e. chip backside), offer direct access to the transistor layers in the Integrated Circuit (IC). Therefore, the transparency of silicon to Near-Infrared (NIR) photons is leveraged to develop new optical FA techniques, like Photon Emission Analysis (PEA), Laser Fault Injection (LFI), Electro-Optical Probing (EOP), and Optical Beam Induced Resistance Change (OBIRCH), based on monitoring emitted/modulated photons from the functional circuit.

While the aforementioned optical techniques were developed for faster FA, their capability of run-time monitoring chip activity risks the exposure of sensitive information stored in the IC. Direct access to bulk silicon in flip-chip packaging and absence of any protection mechanism at chip backside allows an attacker to optically probe the electrical signal without any physical contact. An adversary can scrutinize real-time circuit activity of sequential or combinatorial logic, Physical Unclonable Function (PUF), cache memory, and even true random number generators (TRNG) [1]–[7].

The optical attacks are challenging the confidentiality, availability, and integrity of the assets stored in the chip, by extracting information which is formally proven to be impossible to extract with other physical attacks (e.g. side-channel analysis and fault-injection). Logic locking is a contemporary example of such scenarios where a significant effort is made to protect the design against formal attack approaches like Boolean Satisfiability (SAT) attacks [8], Signal Probability Skey (SPS) attacks [9], bypass attacks [10], and key sensitization [11] attacks. Logic locking appeared as a promising solution against Intellectual Property (IP) piracy. Logic locking is a method of protecting the confidentiality of IP by locking the original circuitry with additional logic elements like XOR gates or multiplexers [12], [13]. The key used for locking the activity of IP is considered as the single barrier between piracy. In recent years, it has been shown that despite provably-secured implementation of locked IP, the locking key can be exposed if the key is accessible from chip backside [14], [15]. The entire attack on locking key can be even completed without access to the gate-level netlist of the chip.

The objectives of this paper are threefold. First, to present a taxonomy of different optical attacks. Second, to identify a variety of optical attack techniques against logic locking and the possible attack methodology. Third, to analyze the benefits and constraints of several countermeasures against optical attacks that have been proposed so far.

This paper is organized as follows: The taxonomy of optical attacks and different logic locking methodologies are discussed in Sec. II and Sec. III, respectively. The security threats imposed by optical attacks on those techniques and attack methodologies are described in Sec. IV. Sec. V investigates the possible countermeasures against backside optical attacks. Finally, we conclude our study in section VI with a focus on the future direction of optical attack detection and avoidance methods.

II. OPTICAL ATTACK APPROACHES

There are three primary optical attack methods depending on the stimulation technique and source of photon emission or modulation (see Tab I): a) Photon Emission Analysis, b) Optical Probing, and c) Laser-Fault Injection.

A. Photon Emission Analysis

PEA is a passive optical attack technique. During the switching of logic states, the transistors implemented in the logic go through the saturation region for a brief period. The charge carriers within the corresponding transistors gain kinetic energy. This energy is released near the channel

TABLE I: Techniques and observable parameters for different optical attack methodologies

Optical Attacks	Classification	Observable Parameters
Photon Emission Analysis	PEA, Picosecond Circuit Analysis (PICA)	Photon emitted during transistor switching
Optical Probing (Electro-optical Analysis)	EOFM, EOP	Reflected photon modulated by electric field and free carrier density in transistors
Laser-fault Injection	-	Switching of transistor caused by laser stimulation

pinch-off region of charge inversion layer in space-charge region, as hot-carrier luminescence [16], [17]. Photons are detected by a Si-CCD or InGaAs detector. With the help of some additional computer processing, a 2-D image can be constructed that maps the switching activity of a Region-of-Interest (RoI). Due to the higher mobility of electrons, the intensity of emitted photons from n-type MOSFET is significantly higher than p-type MOSFET. Therefore, the emission coincides with the switching activity of n-type MOSFET. A variant of PEA, Picosecond image Circuit Analysis (PICA), can provide temporal and spatial information of change in logical state for sequential and combinatorial logic.

B. Optical Probing or Electro-optical Analysis

Electro-optical technique is an active approach for optically probing the transistor state through two well-known approaches – Electro-Optical Probing (EOP) and Electro-Optical Frequency Mapping (EOFM) [18], [19]. EOP involves probing electrical signals on the transistor with an incoherent light source whereas EOFM creates an activity map of the circuitry operating at a certain switching frequency. During optical probing, the laser stimuli is focused on a MOSFET or RoI and gets reflected from different interference in the device, e.g., active region, oxide layer, or interconnect. The amplitude and phase of the injected laser is modulated by the switching electric field and free-carrier density present in the device [20], [21]. The reflected photons are converted into an electrical signal using a photodiode. This electrical signal is fed to a digital sampling oscilloscope or spectrum analyzer depending on the optical probing approach. The oscilloscope averages the electrical signal and synchronizes it with a trigger signal to create a time-domain EOP waveform. The temporal resolution of EOP is usually on the order of tens or hundreds of picoseconds, small enough to probe signals in a modern day System-on-Chip (SoC).

In EOFM, the laser scans the Region of Interest in the Device Under Test (DUT) and the modulated reflected light is evaluated by a spectrum analyzer, which acts as a narrow-band frequency filter [22]. The frequency-filtered values are then sampled for every scanned pixel and used to construct a 2D image using a grayscale or false-color representation to scrutinize spatial activity of different nodes in the circuit [6], [23]. Other approaches for optical probing are Laser Voltage Probing (LVP) and Laser Voltage Imaging (LVI). The LVP and LVI methods are equivalent to EOP and EOFM, respectively, except the light source used for the latter ones are incoherent.

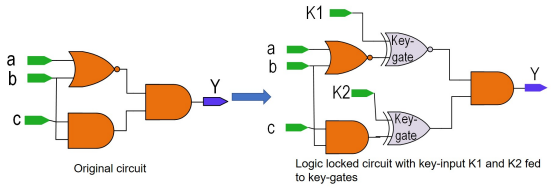


Fig. 1: Simplified example of logic locking method.

C. Laser-fault Injection

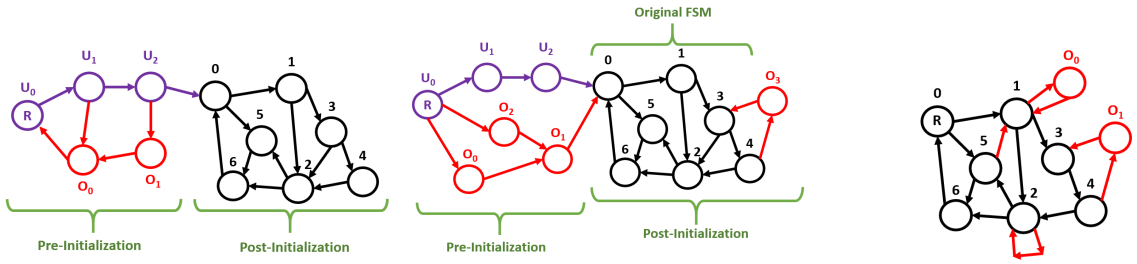
Unlike the observational role of the aforementioned techniques, Laser Fault Injection (LFI) introduces the ability to actually modify the logical state of a target region. LFI relies on the manipulation of an infrared laser with higher energy than silicon's bandgap energy. This property allows for the formation of electron-hole pairs inside the silicon, a phenomenon termed Photoelectric Laser Stimulation (PLS). When the PLS effect is directed towards the source or drain of a transistor in a CMOS circuit, it can flip the CMOS' logical state, introducing a 'fault' into the circuit. The overall success of Laser Fault Injection is not guaranteed because it depends on variables like exposure time and power [2], [24]. However, the ramifications can be powerful when properly executed, like in previous works where faults were injected in embedded microcontrollers and FPGAs.

III. Background on Logic Locking

Optical attacks can be used to expose the security assets protected by the SoC. In this section we will discuss the security threat of optical attacks from a locked IP perspective. There are two prevalent form of logic locking at gate-level: a) Combinational logic locking and b) Sequential or Finite-State-Machine (FSM) logic locking.

A. Combinational Logic Locking

Logic obfuscation, or logic locking, obscures the functionality and structural behaviour of a gate-level implementation of IP cores, to prevent IP reusing or reverse engineering attempts. In combinational logic locking, the IP is locked by inserting additional key-controlled logic gates, called *key-gates* in the design [12] (see Fig. 1). The key can be fed to the key-gates through a set of registers, known as *key-registers* [23]. The key is not available during the fabrication process and is inserted into an NVM (e.g., Flash, EEPROM, or e-fuse) inside the chip before releasing the chip to market or deploying it in the field. The end product of a logic-locked circuit is an entanglement of the original gates and the obfuscation gates, along with signal paths to the tamper-evident memory where the key is stored. Consequently, the correct functionality is hidden from an untrusted foundry during manufacturing.



(a) (b) (c)

Fig. 2: (a)An example HARPOON-Type state space. The U_0, U_1, U_2 in preintitialization state represents the valid path to initiate the functionality of the IP (shown in purple color). Wrong key-sequence will lead the pre-initialization back to the initial U_0 state, (b) an example Interlocking-Type state space. The U_0, U_1, U_2 is still the correct pre-initialization path (shown in purple color). Traversing the proper startup path is important not because it's the only way to access the original FSM, like with HARPOON-Type, but because it unlocks the correct functionality within the original FSM region. Disabling the transition to obfuscation state O_3 is an example of this, (c) an example Entangled-Type state space. New FSM states are directly implemented alongside the functional states of the IP. Hence, obfuscated states are indistinguishable from the functional states.

B. Sequential or FSM Logic Locking

Recall that a Finite State Machine (FSM) is a logical construct representing distinct "states" and some associated transition logic, implemented with flip-flop based "state bits" and combinational blocks. Also recall the idea of "reachability", where the number of states utilized in a given FSM is often far below the total number of states that can be encoded with the FSM's state bits [25], [26].

FSM Logic Locking takes advantage of the low reachability in most FSMs by inserting additional states and state transitions into the state space. These additional states can obscure the original design without adding any functional purpose, thus complicating any reverse engineering and functionality extraction. This is often referred to as State Space Obfuscation (SSO). Three types of State Space Obfuscation will be considered: HARPOON, Interlocking, and Entangled.

a) HARPOON: HARPOON [13] is the first category we will evaluate. HARPOON offers both obfuscation and authentication in designing and manufacturing steps by modifying both the state transition function and the internal logic structures of the design. In HARPOON, the state space is divided into two different operational stages – (a) pre-initialization space and (b) post-initialization space. The pre-initialization space contains a cluster of added states that lead up to the post-initialization space, which is the original, functional region of the FSM locked IP (see Fig. 2a). To navigate to the post-initialization space after reset, the FSM needs the correct input sequence, which can be termed as key-sequence, throughout the pre-initialization stage. The portions of the key are sequentially loaded as part of the Primary Inputs to the transition logic. When the pre-determined key patterns are correct, the state machine follows along the path leading to the first unobfuscated state in the post-initialization section.

b) Interlocking Obfuscation: Interlocking obfuscation [27] implements two separate state space regions, similar to HARPOON's pre-initialization and post-initialization.

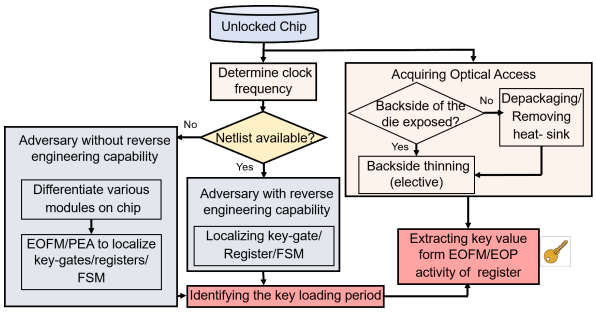


Fig. 3: Simplified illustration of key extraction methodology from logic obfuscated circuitry using optical contactless probing.

The main difference is that in the post-initialization region containing the functional FSM, additional obfuscation states are added. Also, as shown in Fig. 2b, every path in the pre-initialization space leads to entering the original FSM's starting state. However, only one path 'unlocks' the original FSM and allows it to function correctly without the hindrance of those extra obfuscation states.

c) Entangled Obfuscation: Lastly, Entangled Obfuscation [28] presents a newer yet conceptually simpler form of obfuscation. Unlike the previous types, the Entangled form contains only one main region in the state space. Rather than splitting into a startup region and another region with the original FSM, the Entangled type just contains the original FSM states interwoven with additional obfuscation states. This more direct form of obfuscation is a good solution to algorithmic attacks. Ironically, though, it diminishes the circuit to be more easily susceptible to optical attack, particularly through optical probing.

IV. Security Threat of Optical Attack: A Logic Locking Perspective

Previously, the research related to logic locking focused on developing algorithms to protect against attacks based on

formal methods, like SAT attack, key sensitization, and SPS attack. The security of the key itself was completely ignored since the key is assumed to be protected in a read- and tamper-proof memory. The validity of such an assumption can be challenged considering the key signal can be probed easily once the signal propagation path is exposed. For this purpose we can assume that an adversary has access to an unlocked chip. Hence, optical attack based key extraction can be considered an Oracle-guided attack.

A. Attack Methodology

The objective of an adversary is to probe the assets with minimum perturbation in the chip. Therefore, an adversary needs to complete a set of essential steps to acquire access to the locking key. Understanding these steps and optical attack methods will enable us to develop effective and appropriate countermeasures. Fig. 3 shows the essential steps for extracting the key for both combinational and sequential logic locking.

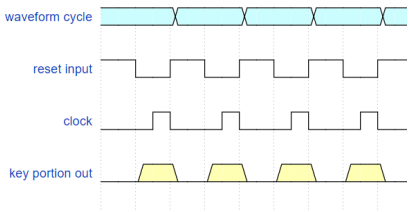
a) Acquiring Optical Access: The attacker needs physical access to the chip. Often, the chip can be easily acquired from the open market or any untrusted entity in the semiconductor supply chain. In optical attacks, an adversary monitors either the photon emitted or modulated due to transistor activity. Therefore, in order to execute optical attacks, an adversary requires direct access to chip backside. Chip backside can be accessed by removing the heat-sink and lids if the device under attack (DUA) is a flip-chip. In non-flip chip, the adversary can remove the packaging material through acid etching or mechanical polishing.

b) Target Localization: In order to extract key values using optical attacks, an adversary can choose the key-delivery unit as an attack surface [14], [23], [29]. Key-delivery unit is a core component consisting of key-gates, registers and corresponding memory reading circuitry [23]. The key-delivery unit can be localized by analyzing the bootup process or run-time monitoring of the chip. Since the locking key is imperative for the functionality of the IC/IP, the key must be available at the key-registers once the secured bootup process is complete [14], [30]. An attacker with gate-level netlist can localize the key-delivery unit through full-blown reverse engineering.

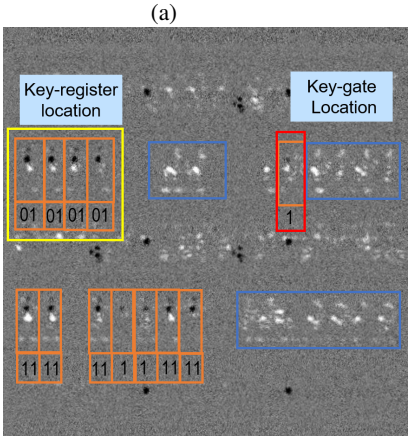
c) Optical Attack: An adversary can use PEA [31], optical probing [14], [23], or LFI attack [15] to extract the locking key. A successful optical attack requires a laser source with variable wavelengths for laser stimulation and an InGaAs detector for photon emission analysis. Recent advancements in FA instruments have incorporated the laser source with different wavelength and PEA capability to provide a single solution for all optical debugging techniques [22].

B. Security Assessment of Combinational Logic Locking Against Optical Probing.

To evaluate the vulnerability of logic locking against optical probing, we assume that the locked chip is available. The adversary can localize the key-gates/registers from PEA and EOFM analysis of the secure bootup process of the IC [14]. Once the location of the key-gates and key-registers are localized, an attacker can launch either EOFM or EOP measurement to extract the key bits.



(a)



(b)

Fig. 4: (a)The chip is reset at a certain frequency in a loop. The EOFM signal is collected at the reset frequency, (b) The EOFM activity at clock frequency and reset frequency where, black and white dots represents clock and logic element activity, respectively. The value stored in each register is mentioned at the bottom of the corresponding register. The registers in the yellow box represents the key-register location and red box represents the register responsible for the reset signal.

As shown in Fig. 4b, the chip gets forced to repeatedly reset in a loop, with a reset frequency that will be the target frequency in EOFM measurement. The key bit values of logical '1' appear as active nodes in EOFM measurement since the corresponding registers toggle at the frequency of the reset loop. For logical '0's, the nodes appear as inactive nodes in EOFM image. Thus, the key bits of each key-registers/gates can be extracted using EOFM analysis. Unlike EOFM where more than one key-bit can be extracted through a single measurement, EOP requires separate measurements for each key-bit.

C. Security Assessment of Sequential Logic Locking Against Optical Probing

The FSM locked circuit is considered broken once an adversary localizes the pre-initialization region and obtains the key input sequence used for pre-initialization, or for the Entangled type, simply obtains the key input.

a) Pre-initialization Space and Key Localization: Since HARPOON implements pre-initializion with additional state-

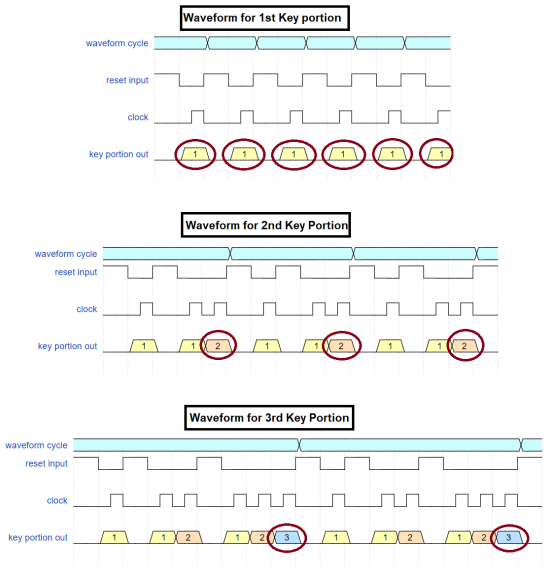


Fig. 5: The reset signal going in to the chip is forced on and off with different input waveforms. For the first key portion, simply alternating the reset signal symmetrically is enough, for the same reasons as the logic locking waveform. Subsequent key portions, however, have to be "built up" to. Notice how the frequency of each target key portion being loaded always matches the frequency of the entire waveform cycle.

elements and combinational elements, an adversary with access to IP netlist can focus on identifying the registers implemented with the pre-initialization FSM. Such registers can be identified using gate-level reverse engineering methods such as RELIC [32] and strongly connected components (SCC) [33] algorithm. An adversary without access to gate-level netlist can use PEA during secure bootup and optical image of die to identify the possible FSM locations.

b) Key Extraction: Once the localization of the registers involved in pre-initialization is determined, in principle, the attacker can use either EOFM or EOP measurement to extract the key value from an unlocked chip. However, due to low signal-to-noise ratio of optical probing signal, multiple optical probing measurements are necessary. This can be achieved by resetting the chip in a loop manner. The exact time to trigger and hold the reset signal depends on the key availability at the key-register. Here we discuss two different scenarios for key extraction using optical probing,

1) **Scenario-1:** All the key bits are fed concurrently to the the key-registers during secure bootup of the IP.
2) **Scenario-2:** In this scenario, the key bits are available at the state-element input once the previous pre-initialization state is unlocked using the correct key portion.

HARPOON and Interlocking State Space Obfuscation fall under scenario 2, because of the use of the pre-initialization space. Entangled-Type falls under scenario 1, similar to combinational logic locking, because the reset state is the same as the original FSM and the obfuscation states entangled throughout it are likely unlocked right away.

In scenario 1, an adversary can optically probe all the key-registers simultaneously in a straight forward manner according to the method described in Sec. IV-B. However, the key-registers can not be probed concurrently in scenario-2. As shown in Fig. 5, the adversary can keep the circuit enabled for longer periods of time in each iteration to build up to each key portion. For example, consider the 2nd key portion. If each waveform cycle simply lets the FSM fetch up to the 2nd key portion repeatedly, then there would be no distinguishable frequency between portion 1 and 2 being loaded. Thus, each waveform cycle consists of multiple resets, where the reset signal is held low for different lengths to iterate up to the target key portion. Overall, there will be a separate repeated waveform utilized per pre-initialization state leading up to the original FSM.

V. Potential Countermeasures

Optical attacks can be only prevented by protecting the chip backside from intrusion or increasing the time-cost of optical attacks. At the packaging level, such protection can be provided by adding active opaque layers to the backside of the chip. As such layers can easily be removed, an active monitoring scheme must be implemented to detect an adversarial attack [34].

At the device level, photo sensors can be deployed to detect an attack attempt. Since thermal lasers are widely used for optical probing, an adversary can circumvent the photo sensors. Nonetheless, the thermal stimulation introduces temperature and current variations in the circuit, which can influence circuits, such as ring-oscillators (ROs) [35]. In this case, implementing ROs as a probing protection scheme can generate an anti-tamper reaction in the chip to protect the locking keys. In [36] nanopyramid structures are implemented in selective areas inside the chip to mitigate optical probing attacks by scattering the reflected laser beam, and consequently, scrambling the measurements of the register contents.

Randomizing the state of the key-register or clock frequency during the boot-up of locked IP can be a solution against optical probing. A true random number generator (TRNG) can be used to store random values at the key-register. One should note that, storing random values in the key-register may introduce reliability issues for the chip. Therefore, additional control circuitry is require to store the random values during the inactive state of the corresponding IPs. However, integrating TRNG in the circuit may introduce additional area and delay overhead to the chip. In addition, untrusted foundries can localize and remove the TRNG through reverse engineering and circuit edit, respectively [37].

VI. Conclusion

In this study, a comprehensive study about different optical attack techniques and corresponding security threats of logic locked chips are presented. Optical attack methods

exploit the lack of security at the chip backside for run-time monitoring and raiding the chip. Therefore, developing detection and prevention based countermeasures can be used to protect the locking key. We have also discussed possible countermeasures suitable for logic locking attacks and the limitations of those protection schemes.

REFERENCES

[1] A. Schlösser, D. Nedospasov, J. Krämer, S. Orlic, and J.-P. Seifert, "Simple photonic emission analysis of aes," in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2012, pp. 41–57.

[2] S. Tajik, H. Lohrke, F. Ganji, J.-P. Seifert, and C. Boit, "Laser fault attack on physically unclonable functions," in *2015 workshop on fault diagnosis and tolerance in cryptography (FDTC)*. IEEE, 2015, pp. 85–96.

[3] F. Courbon, P. Loubet-Moundi, J. J. Fournier, and A. Tria, "Increasing the efficiency of laser fault injections using fast gate level reverse engineering," in *2014 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*. IEEE, 2014, pp. 60–63.

[4] S. P. Skorobogatov and R. J. Anderson, "Optical fault induction attacks," in *International workshop on cryptographic hardware and embedded systems*. Springer, 2002, pp. 2–12.

[5] H. Lohrke, S. Tajik, T. Krachenfels, C. Boit, and J.-P. Seifert, "Key extraction using thermal laser stimulation," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 573–595, 2018.

[6] 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*. ACM, 2017, pp. 1661–1674.

[7] M. T. Rahman, S. Tajik, M. S. Rahman, M. Tehranipoor, and N. Asadizanjani, "The key is left under the mat: On the inappropriate security assumption of logic locking schemes," Cryptology ePrint Archive, Report 2019/719, 2019, https://eprint.iacr.org/2019/719.

[8] P. Subramanyan, S. Ray, and S. Malik, "Evaluating the security of logic encryption algorithms," in *Hardware Oriented Security and Trust (HOST), 2015 IEEE International Symposium on*. IEEE, 2015, pp. 137–143.

[9] M. Yasin, B. Mazumdar, O. Sinanoglu, and J. Rajendran, "Removal attacks on logic locking and camouflaging techniques," *IEEE Transactions on Emerging Topics in Computing*, 2017.

[10] X. Xu, B. Shakya, M. M. Tehranipoor, and D. Forte, "Novel bypass attack and bdd-based tradeoff analysis against all known logic locking attacks," in *International Conference on Cryptographic Hardware and Embedded Systems*. Springer, 2017, pp. 189–210.

[11] J. Rajendran, Y. Pino, O. Sinanoglu, and R. Karri, "Security analysis of logic obfuscation," in *Proceedings of the 49th Annual Design Automation Conference*. ACM, 2012, pp. 83–89.

[12] J. A. Roy, F. Koushanfar, and I. L. Markov, "Epic: Ending piracy of integrated circuits," in *Proceedings of the conference on Design, automation and test in Europe*. ACM, 2008, pp. 1069–1074.

[13] R. S. Chakraborty and S. Bhunia, "Harpoon: an obfuscation-based soc design methodology for hardware protection," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 28, no. 10, pp. 1493–1502, 2009.

[14] M. T. Rahman, S. Tajik, M. S. Rahman, M. Tehranipoor, and N. Asadizanjani, "The key is left under the mat: On the inappropriate security assumption of logic locking schemes," in *Conference on IEEE Int. Sym. on Hardware Oriented Security and Trust (HOST)*, 2020.

[15] A. Jain, M. T. Rahman, and U. Guin, "Atpg-guided fault injection attacks on logic locking," in *Conference on IEEE Int. Conf. on Phy. Assurance and Inspection of Electronics (PAINE)*, 2020.

[16] A. Schlösser, D. Nedospasov, J. Krämer, S. Orlic, and J.-P. Seifert, "Simple photonic emission analysis of aes," in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2012, pp. 41–57.

[17] M. T. Rahman and N. Asadizanjani, "Backside security assessment of modern socs," in *2019 20th International Workshop on Microprocessor/SoC Test, Security and Verification (MTV)*. IEEE, 2019, pp. 18–24.

[18] Z. Song and L. Safran, "Lvi and lvp applications in in-line scan chain failure analysis," *Electronic Device Failure Analysis*, vol. 18, no. 4, pp. 4–14, 2016.

[19] W. M. Yee, M. Paniccia, T. Eiles, and V. Rao, "Laser voltage probe (lvp): A novel optical probing technology for flip-chip packaged microprocessors," in *Proceedings of the 1999 7th International Symposium on the Physical and Failure Analysis of Integrated Circuits (Cat. No. 99TH8394)*. IEEE, 1999, pp. 15–20.

[20] N. Vashistha, M. T. Rahman, O. P. Paradis, and N. Asadizanjani, "Is backside the new backdoor in modern socs?" in *2019 IEEE International Test Conference (ITC)*. IEEE, 2019, pp. 1–10.

[21] U. Kindereit, "Fundamentals and future applications of laser voltage probing," in *2014 IEEE International Reliability Physics Symposium*. IEEE, 2014, pp. 3F–1.

[22] H. Photonics, "Emission Microscopy: Phemos-1000," https://www.hamamatsu.com/resources/pdf/sys/SSMS0003E_PHEMOS1000.pdf, accessed:2018-04-26.

[23] M. T. Rahman, M. S. Rahman, H. Wang, S. Tajik, W. Khalil, F. Farahmandi, D. Forte, N. Asadizanjani, and M. Tehranipoor, "Defense-in-depth: A recipe for logic locking to prevail," *Integration*, vol. 72, pp. 39–57, 2020.

[24] J.-M. Schmidt, M. Hutter, and T. Plos, "Optical fault attacks on aes: A threat in violet," in *2009 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*. IEEE, 2009, pp. 13–22.

[25] S. Amir, B. Shakya, X. Xu, Y. Jin, S. Bhunia, M. Tehranipoor, and D. Forte, "Development and evaluation of hardware obfuscation benchmarks," *Journal of Hardware and Systems Security*, pp. 1–20, 2018.

[26] T. Hoque, R. S. Chakraborty, and S. Bhunia, "Hardware obfuscation and logic locking: A tutorial introduction," *IEEE Design & Test*, 2020.

[27] A. R. Desai, M. S. Hsiao, C. Wang, L. Nazhandali, and S. Hall, "Interlocking obfuscation for anti-tamper hardware," in *Proceedings of the eighth annual cyber security and information intelligence research workshop*, 2013, pp. 1–4.

[28] T. Meade, Z. Zhao, S. Zhang, D. Pan, and Y. Jin, "Revisit sequential logic obfuscation: Attacks and defenses," in *2017 IEEE International Symposium on Circuits and Systems (ISCAS)*. IEEE, 2017, pp. 1–4.

[29] S. Engels, M. Hoffmann, and C. Paar, "The end of logic locking? a critical view on the security of logic locking." *IACR Cryptol. ePrint Arch.*, vol. 2019, p. 796, 2019.

[30] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[31] S. Tajik, D. Nedospasov, C. Helfmeier, J.-P. Seifert, and C. Boit, "Emission analysis of hardware implementations," in *2014 17th Euromicro Conference on Digital System Design*. IEEE, 2014, pp. 528–534.

[32] T. Meade, Y. Jin, M. Tehranipoor, and S. Zhang, "Gate-level netlist reverse engineering for trojan detection and hardware security," in *The IEEE International Symposium on Circuits and Systems (ISCAS)*, 2016, pp. 1334–1337.

[33] R. Tarjan, "Depth-first search and linear graph algorithms," *SIAM journal on computing*, vol. 1, no. 2, pp. 146–160, 1972.

[34] E. Amini, A. Beyreuther, N. Herfurth, A. Steigert, B. Szyszka, and C. Boit, "Assessment of a chip backside protection," *Journal of Hardware and Systems Security*, vol. 2, no. 4, pp. 345–352, 2018.

[35] S. Tajik, J. Fietkau, H. Lohrke, J.-P. Seifert, and C. Boit, "Pufmon: Security monitoring of fpgas using physically unclonable functions," in *2017 IEEE 23rd International Symposium on On-Line Testing and Robust System Design (IOLTS)*. IEEE, 2017, pp. 186–191.

[36] H. Shen, N. Asadizanjani, M. Tehranipoor, and D. Forte, "Nanopyramid: An optical scrambler against backside probing attacks," in *ISTFA 2018: Proceedings from the 44th International Symposium for Testing and Failure Analysis*. ASM International, 2018, p. 280.

[37] M. T. Rahman, Q. Shi, S. Tajik, H. Shen, D. L. Woodard, M. Tehranipoor, and N. Asadizanjani, "Physical inspection & attacks: New frontier in hardware security," in *2018 IEEE 3rd International Verification and Security Workshop (IVSW)*. IEEE, 2018, pp. 93–102.