SPARTA-COTS: A Laser Probing Approach for Sequential Trojan Detection in COTS Integrated Circuits

Andrew Stern*, Dhwani Mehta*, Shahin Tajik*, Ujjwal Guin†, Farimah Farahmandi*, Mark Tehranipoor*
Department of Electrical and Computer Engineering, University of Florida*
Department of Electrical and Computer Engineering, Auburn University†
{andrew.stern, dhwanimehta, stajik}@ufl.edu, ujjwal.guin@auburn.edu, {farimah, tehranipoor}@ece.ufl.edu

2020 IEEE Physical Assurance and Inspection of Electronics (PAINE) | 978-1-7281-6121-1/20/$31.00 ©2020 IEEE | DOI: 10.1109/PAINE49178.2020.9337728

***Abstract*—Rapid advancements in integrated circuit (IC) technology have been led by the private sector. This leadership has resulted in a widespread dependence of commercial-off-the-shelf (COTS) components in our electronic systems. However, being dependent upon potentially compromised hardware serves as a threat to our security. Hardware Trojans, which can extract sensitive information and disrupt system operations, can be inserted into COTS ICs by untrusted design and fabrication facilities. Checking for the existence of Trojans using conventional methods requires a complex test process and design-level modifications, which requires trusted design information, making them unsuitable for COTS components. On the other hand, for a high confidence detection of Trojans, an exhaustive inspection may be required using destructive reverse-engineering techniques. However, such methods are quite expensive, not applicable to all chips due to their destructive nature, and very time-consuming. In this work, we propose SPARTA-COTS, a non-destructive laser probing approach for Trojan detection in COTS ICs, which detects sequential hardware Trojans by leveraging existing scan chain architecture. SPARTA can differentiate between benign scan flip-flops and malicious sequential hardware Trojans by creating a 2-dimensional frequency activity map of the backside silicon at the clock and scan input frequencies using electro-optical frequency mapping (EOFM). Consequently, SPARTA is capable of confidently identifying Trojan flip-flops using image processing techniques. To validate our claims, we present automated detection results on a 28 nm device.**

***Index Terms*—Sequential Trojan Detection, Commercial-off-the-Shelf, ASIC, Optical-Probing, Hardware Security**

I. Introduction

The microelectronics supply chain has become increasingly globalized. As a result, the need to authenticate untrusted hardware has risen. Commercial-off-the-shelf (COTS) components, designed and manufactured around the world, are being deployed within critical systems and infrastructure which require the utmost reliability. Hardware Trojans, i.e., malicious modifications introduced into a circuit, pose a threat to the safety of those dependent upon these critical systems. Hardware Trojans are capable of extracting privileged information from ICs, enabling access through covert channels, and even disabling device functionality [1]–[3]. As integrated circuit (IC) production is rapidly approaching a *zero-trust* threat model, where no single entity can be trusted, the potential threat of hardware Trojans warrants an effective response.

The threat of hardware Trojan insertion has inspired research across the pre-silicon and post-silicon life-cycle for the purpose of Trojan detection, design-for-trust, and split manufacturing for trust (i.e., Trojan prevention) [3]. Proposed detection (validation) and prevention methods, such as design-for-trust and split manufacturing, attempt to, for instance, increase controllability and observability of specific nets by adding test points to the original design or separating design elements to protect the full design [4]–[7]. These methods typically incur a high cost, design-constraint penalty, or can introduce additional vulnerabilities that can be exploited by attackers to cause integrity and confidentiality violations to a design's critical information. Additionally, pre-silicon detection and prevention methods cannot be guaranteed with COTS ICs and require implementation by the COTS design house. Alternatively, post-silicon detection methods have been proposed to verify authenticity.

Existing post-silicon Trojan detection methods rely on destructive reverse engineering, applying complex test processes, or comparisons against golden ICs [8]–[11]. Destructive techniques require detailed delayering and imaging of a device-under-test (DUT), which can be error-prone, costly, and time-consuming. On the other hand, logic-based approaches rely upon the application of parametric and logical tests [7]. In this case, such testing methods require trusted circuit design information, small-scale ICs, or Trojan trigger activation and propagation of payload to an observable output (e.g., primary output or scan chain). Existing non-destructive side-channel techniques require golden references of fabricated ICs [12]. This condition cannot be met with a realistic threat model, as the verifying party will not always have a golden sample of their COTS IC. Besides, such methods do not scale well to larger devices and typically cannot cover low-probability (hard-to-detect) and sequential Trojans. Notably, sequential Trojans may require propagation through a complex state space before reaching a possible activation condition. Therefore, generating tests that activate hidden Trojans is extremely difficult.

Our Contribution. In this work, we introduce SPARTA-COTS, a laser probing approach using electro-optical frequency mapping (EOFM) to *non-destructively* detect sequential Trojans without design-for-trust nor prior knowledge of the COTS component. Moreover, since our laser probing approach, SPARTA, requires only a clock signal and, in this scenario, a single repeating scan input pattern, we only need to leverage existing circuit test infrastructure to determine if malicious sequential elements exist outside of the scan chain. To validate SPARTA-COTS, we conduct experiments on Trojan benchmarks implemented on a commercial 28-nm FPGA and show the automated detection of Trojans. It should be noted that although we utilized an FPGA for our proof-of-concept, the method is applicable to ASICs as well (see Section III).

II. Background

A. Sequential Trojans

Hardware Trojans are defined as malicious modifications to a circuit design. This malicious circuitry can be identified as combinational (i.e., combinational logic gates only) or sequential (i.e., utilizing memory elements). Combinational Trojans are assumed to be placed at low switching probability nodes to avoid activation, and several examples have been generated and made publicly available on Trust-Hub [13], [14]. Additionally, sequential hardware Trojans represent the most diverse set of malicious circuit modifications. Sequential Trojans may be triggered synchronously, asynchronously, a hybrid approach, or from rare sequences [15]. This broad area of powerful Trojans is likely to avoid detection from conventional testing techniques as random tests are unlikely to trigger them.

On the other hand, sequential triggering mechanisms are the most sophisticated attack option for untrusted designers and foundries [3], [4]. As ICs further scale, sequential Trojans are ideal for hiding their impact during standard IC testing. Often the test methodology for an IC aims to identify faults (e.g., stuck-at) which may arise from the manufacturing process, but these tests may also be used to target combinational Trojan triggers. However, sequential Trojans may not be triggered during such testing due to the potential progression through various states to a specific target location. This multi-cycle path makes the detection of sequential Trojans increasingly difficult and unlikely. Detection techniques have been previously proposed, although they often require advanced circuit knowledge, modifications at the design phase, or the activation of the Trojan for detection [16]–[18].

B. Hardware Trojan Detection

Trojan detection in ICs can be generalized as destructive or non-destructive. Destructive approaches yield high-confidence results, but render the DUT unusable after processing [19]–[21]. Non-destructive approaches allow for use of the ICs after they have been analyzed, however traditionally these methods have lower confidence levels and require device-specific input patterns to generate the desired circuit activity [9], [10], [12], [22]. Given the lack of information available while working with COTS components, structural pattern information will be difficult to derive without full IC reverse engineering.

Non-destructive optical side-channel based Trojan detection techniques have been previously proposed in [9], [10]. These techniques attempt to identify combinational Trojans by measuring photon emission from the backside silicon when specific test patterns were applied. By using a sensitive temporally-aware photodetector, *combinational* logic was identified on a 90 nm technology node. The authors then compared their measured emissions against a golden IC layout which had been pre-processed to approximate the expected results from experimental measurements. Unlike SPARTA, these techniques rely on extensive test patterns to activate all components within the IC. SPARTA does not require complex test pattern generation for measurement and does not require temporal alignment to collect results. Additionally, photon emission techniques create additional challenges due to aggressive device scaling, as emissions are proportional to the supply voltage of a chip [10].

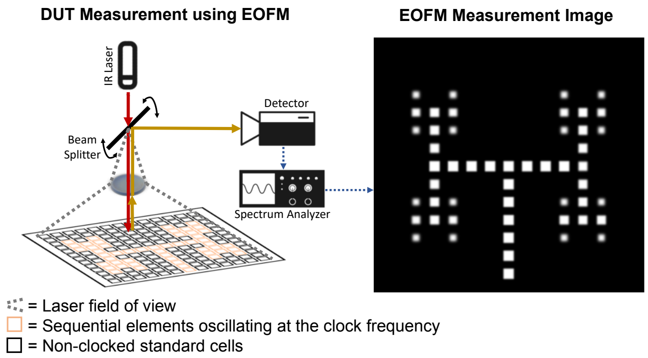
DUT Measurement using EOFM
EOFM Measurement Image
IR Laser
Detector
Beam Splitter
Spectrum Analyzer
⁚⁚ = Laser field of view
□ = Sequential elements oscillating at the clock frequency
□ = Non-clocked standard cells

Fig. 1. EOFM measurement overview depicting IC backside optical probing and expected measurement image.

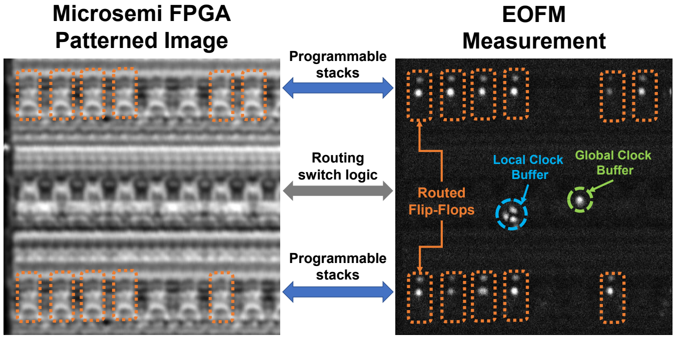

Fig. 2. Laser patterning and EOFM measurements of a 28-nm Microsemi PolarFire FPGA.

C. Electro-Optical Frequency Mapping (EOFM)

Figure 1 illustrates the principle behind the EOFM measurement technique [23]. An infrared laser passing through an optical assembly is incident upon the backside silicon of an IC. Silicon is transparent to infrared wavelengths, and hence, the laser penetrates the silicon substrate and reflects off of the active layer. This reflected light is reflected off of a beam splitter and is measured with a photodetector. The frequency information of the current passing through the cell under the laser is extracted within the reflected light. This information is processed within a spectrum analyzer, which reports the amplitude of the frequency band of interest back to the measurement computer. To create a mapping of the entire DUT, the beam splitter makes subtle adjustments to scan

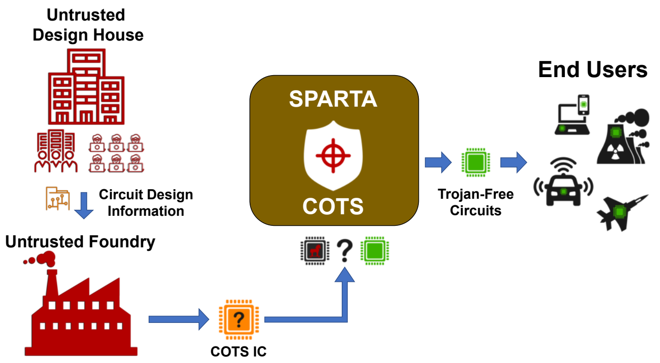

Fig. 3. SPARTA-COTS overview with untrusted COTS components.

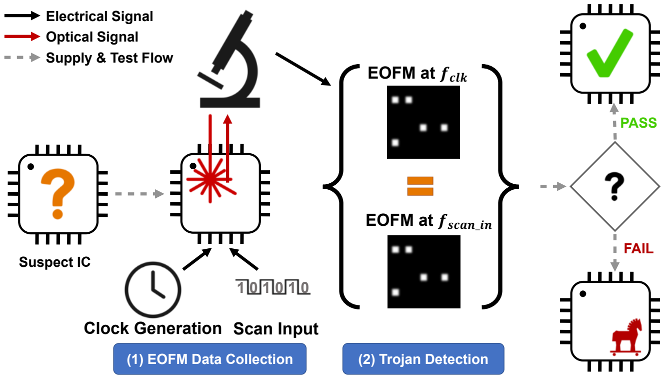

Fig. 4. SPARTA-COTS approach showing: (1) EOFM measurement of a suspect IC at both clock and scan input frequencies. (2) Automated Trojan detection using both EOFM measurements to assess IC authenticity.

the laser across the visible area. These amplitudes are then stitched together to form a frequency map with bright spots which correlate to high current cells at a given frequency. The EOFM overview image (shown in Figure 1) demonstrates the intensity differences between various types of cells within an IC. A simple H-clock tree example is shown with decreasing current flow as the global routing approaches local routing. Figure 2 depicts actual laser patterning and EOFM results and an introduction to the structure of the FPGA backside.

III. SPARTA-COTS Overview

A. Threat Model

COTS integrated circuits are generally produced by untrusted designers and foundries, and handled by untrusted distributors. Figure 3 shows a simplified view of the COTS supply chain. The IC design house, and their corresponding third-party intellectual property (3PIP) vendors, are typically scattered around the world with little insight into IC development. This potentially compromised design file is transferred to an untrusted foundry to fabricate the COTS ICs. Since the foundry needs to manufacture the ICs, they have full visibility into the IC design files and have the ability to insert hardware Trojans by directly modifying the circuit structure. Sequential Trojans can be extremely difficult to detect as traditional techniques require the Trojan to be triggered. We assume that at least one sequential element (flip-flop) is outside of the scan chain. The rational behind this assumption is that a sequential Trojan with its flip-flops in the scan chain would provide high visibility, hence easier detection. As a result, here we assume the attacker will keep components of a sequential Trojan outside of the scan chain architecture. This assumption is mirrored by the sequential Trojan implementations found in the Trust-Hub benchmarks, a subset of which are used in this experiment.

B. Our Approach

SPARTA-COTS combats sequential Trojans in COTS systems by identifying the malicious sequential elements without requiring the Trojan to be triggered. To do this, the laser probing technique EOFM is used to collect data across two different frequencies, and image processing techniques are used to automatically detect Trojans in the collected data set. Figure 4 shows the flow by which a suspect DUT is authenticated.

1) EOFM Data Collection: The suspect IC is positioned under the microscope objective, powered on, and the clock is provided to the circuit. Assuming clock gating is not implemented, the IC clock frequency propagates throughout all sequential elements of the DUT. First, using EOFM targeted at the clock frequency, a map of all sequential elements within the circuit, both benign and malicious, are identified. Next, the suspect IC is powered on and put into scan mode, as seen in Figure 4 (1), with both the clock and scan inputs provided to the circuit. While providing an oscillating input of alternating 1's and 0's, a new frequency can be derived. For example, with a clock frequency of 50MHz, a scan input pattern of repeated 101010. . . will effectively create a square wave at 25MHz (i.e., half of the clock frequency). This oscillating pattern provides a second reference point that identifies all scan flip-flops connected to the scan chain. The next stage processes these two measurements to determine the locations of the sequential Trojans.

2) Automated Trojan Detection: To determine the location of sequential Trojans within the DUT both EOFM images must be compared, as seen in Figure 4 (2). In an ideal scenario, performing a direct comparison between the two frequency measurements should determine the location of the sequential Trojans as all scan flip-flops should contain both frequencies. However, various components such as global and local clock buffers will be present in the EOFM clock measurement, but rightfully missing from the scan input frequency measurement. For accurate and automated detection, image processing techniques are used to identify flip-flops and differentiate them from other circuit elements.

To confidently detect sequential Trojans the raw measurement data is first pre-processed [24]. The active flip-flops (high-intensity spots) are segmented out from the background noise for further analysis. To extract this information, a series of techniques are used as seen in Figure 5. Histogram equalization, which takes the most frequent intensity values and stretches them throughout the image, causes the features (e.g.,

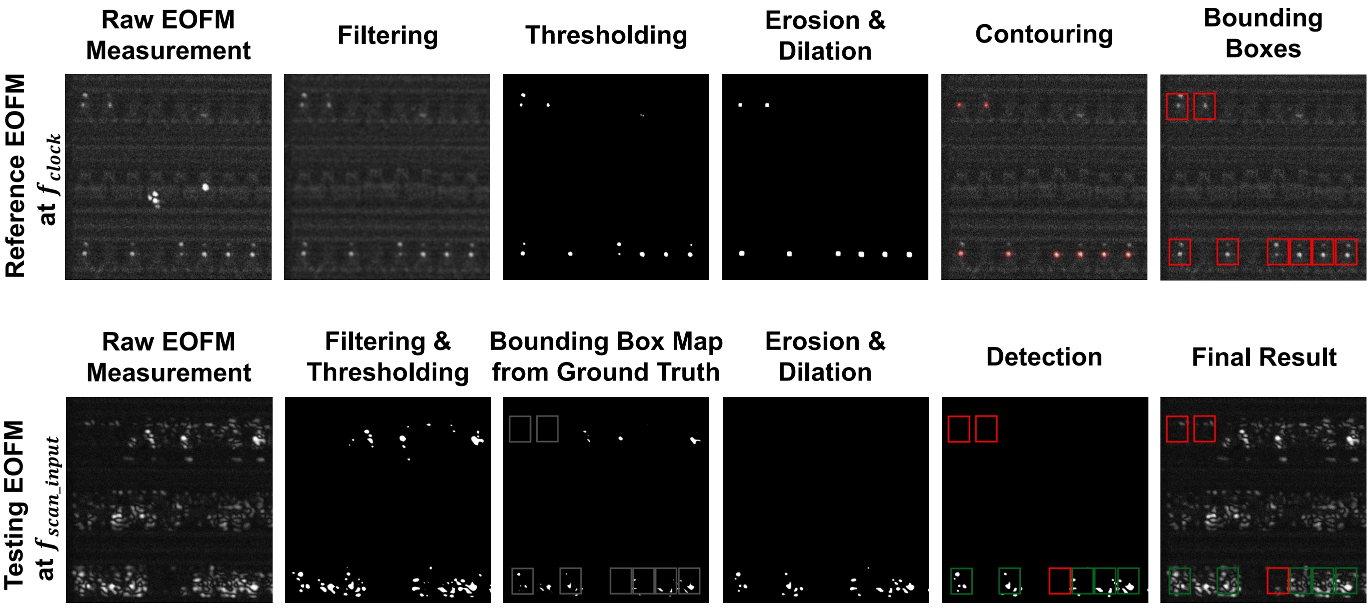

Fig. 5. Image pre-processing and automated hardware Trojan detection using both EOFM measurements.

flip-flop responses) to have a better contrast when compared to the background. Next, a Gaussian filter with a kernel size of seven by seven is used to remove all unwanted white noise. A median filter, with a kernel size of three by three, is applied to smooth the image to preserve edges and to remove any remaining fine background noise. Thresholding converts the grayscale image into a binary image. This eliminates the black background and segments the active flip-flop regions in the images. Finally, after thresholding, erosion and dilation are performed iteratively to clean up the image [25].

After pre-processing the measurements, connected component analysis is used to isolate potential true positives. After this analysis, only high intensity points will remain, and a mask will be generated to store them. Each of these regions must be labeled to automate the remainder of the processing. Here, each of the unique labels is iterated over. If the label is 0 (background) we ignore it, if not we generate a mask only for that label. Next, contours, which join all points along a boundary with the same intensity, are identified and can be used for object detection, recognition, and shape analysis. Once the contours are formed for the regions of interest, bounding boxes (rectangles) are drawn around the regions. The x, y coordinates as well as the width and height of the bounding boxes are stored for processing during the next steps. These bounding boxes from the clock frequency EOFM measurement are mapped to the scan input EOFM measurement for detection. Once this mapping is complete, the intensity values within the bounding boxes are analyzed. This is done by calculating the bright pixel values inside the bounding boxes. After the pixel values are calculated for both EOFM measurement images, a difference between them is taken. To determine if a flip-flop region should be labeled as a Trojan flip-flop (red) or scan flip-flop (green), a threshold range is set. If the calculated difference is greater than the threshold the region is labeled as a Trojan, and if the difference is within the threshold range it is labeled as non-malicious.

IV. Experimental Results

For a proof-of-concept, a 28-nm Microsemi PolarFire FPGA was used as the DUT. This FPGA was specifically chosen as it has the closest physical layout to an ASIC. The circuit representation maintains a similar standard cell style design, in which, flip-flops, buffers, and logic gates can be placed. The selected Microsemi FPGA does differ from an ASIC as the routing and logic functions are programmable. However, the way the circuit is represented, contains stacks of two buffers, two flip-flops, and two logic gates. Hence, the main difference between the stack structure and ASIC designs is that each stack cell contains two separate instances of the flip-flops we are searching for. This emulates a more dense technology node that requires signal amplitude-based analysis techniques to properly evaluate the circuit functionality.

To demonstrate the capabilities of SPARTA, three benchmarks from Trust-Hub were selected. The s1423_T607, s13207_T619, and s15850_T609 represent small, medium, and large benchmarks respectively. The processed EOFM measurements for the small benchmark are shown in Figure 6. The red boxes in Figure 6 (a) identify the physical location of the suspect flip-flops. The blue region illustrates the effective filtering to remove irrelevant elements such as the local and global clock buffers formerly seen in Figure 2. Figure 6 (b) shows the EOFM response of the same area, but at the 25MHz oscillation frequency of the scan input pattern. This measurement provides significantly more extraneous information, since in addition to the flip-flop transistors, there are also logic gates passing values throughout the circuit due to the scan

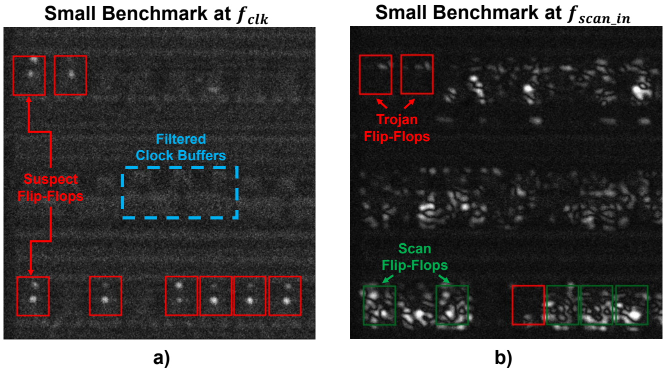

Fig. 6. Processed EOFM images of the small s1423_T607 Trojan benchmark with: (a) Suspect flip-flop identification on the clock frequency EOFM measurement with filtered clock buffers. (b) Trojan detection results on the scan input frequency EOFM measurement.

input patterns. As previously mentioned, the programmable stacks are highly dense structures which include six separate programmable items. Despite this fact, information can still be extracted, and should be further simplified when conducted on an ASIC with dedicated flip-flop cells. The green boxes in Figure 6 (b) represent authentic scan flip-flops, as expected within Trojan-free ICs. However, the red boxes signify Trojan flip-flops which are disconnected from the scan chain.

The automated Trojan detection results results for the medium and large benchmarks are shown in Figure 7. The detection process was made more difficult for these examples as the area constraints within Microsemi Libero IDE were narrowed. This created significant activity throughout the device with nearly all resources within the target region being allocated. Figure 7 (a) shows the correct identification of the sequential Trojans despite the additional noise. Further, Figure 7 (b) shows the results of the large benchmark maintaining a 100% detection accuracy across the 3 benchmarks. Trojan detection within the medium and large benchmarks overcame the added background noise due to increased activity, despite the white balance adversely effecting the depiction of the circuit response. The ability to identify Trojans despite these challenges shows promise for detection at technology nodes below the optical limitations of the current EOFM hardware.

The larger s15850 benchmark is also shown in Figure 8. Here, the Libero IDE layout is shown to demonstrate how the implemented circuits look within the design environment and how they correlate to the measured images. The IDE representation of the overall layout is shown along with a zoomed in region corresponding to the sequential Trojan location and EOFM image. The dotted outlined areas represent programmable stacks that contain programmed flip-flops, as denoted by yellow highlighting within the IDE. The combinational logic, denoted by blue and gates, are all programmed and thus are seen in yellow as well rather than the default off coloration of black. Within the IDE representation all Trojan flip-flops have been highlighted in white to visually differentiate them. The objective of our detection methods is shown by the manually placed red and green dotted outlines that utilize both EOFM images and identify scan flip-flops (green) and Trojan flip-flops (red). The flip-flop placement and Trojan detection results directly match the automated processing results shown in Figure 7 (b). Overall, SPARTA was able to achieve a 100% detection accuracy across all 3 Trojan benchmarks, and the ample feature sizes suggest compatibility with smaller technology nodes as well.

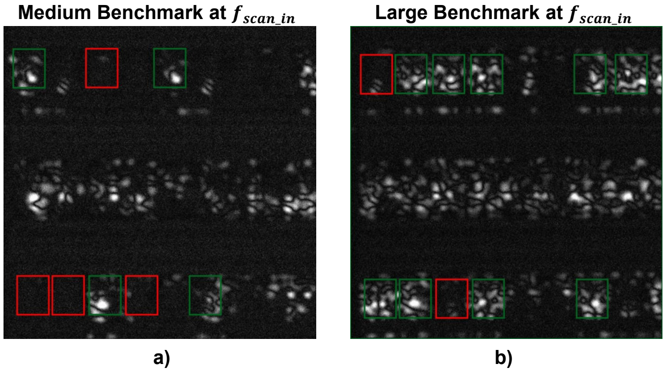
Medium Benchmark at f_{scan_in}
a)
Large Benchmark at f_{scan_in}
b)

Fig. 7. Processed EOFM images with Trojan detection results showing: (a) Medium s13207_T619 Trojan benchmark. (b) Large s15850_T609 Trojan benchmark.

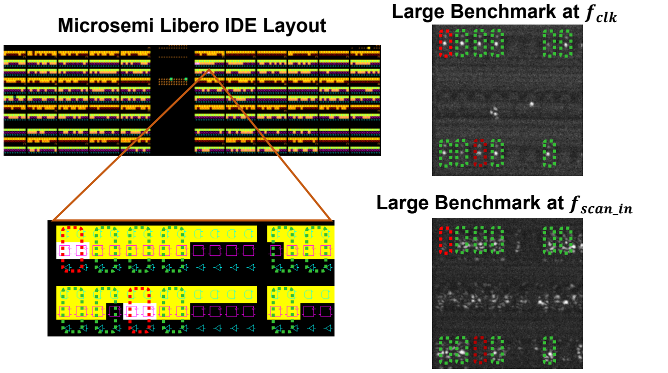
Microsemi Libero IDE Layout
Large Benchmark at f_{clk}
Large Benchmark at f_{scan_in}

Fig. 8. Sample IDE layout to EOFM measurement mapping on large s15850_T609 benchmark.

V. Conclusion

Authenticating COTS electronics is essential to creating trustworthy critical systems. SPARTA-COTS provides a non-destructive, spatially aware detection method for identifying sequential Hardware Trojans in such components. By leveraging existing clock trees and scan infrastructure within ICs, no prior knowledge of the internal circuit structure is necessary. By comparing two EOFM images of the clocked elements and scan elements respectively, sequential Trojan flip-flops outside of the scan chain can be identified. The potential for scalability is shown by implementing automated detection for both of the measurement images, with time scaling linearly with die size.

References

[1] M. Tehranipoor and F. Koushanfar, "A survey of hardware trojan taxonomy and detection," *IEEE design & test of computers*, vol. 27, no. 1, pp. 10–25, 2010.

[2] M. Potkonjak, A. Nahapetian, M. Nelson, and T. Massey, "Hardware trojan horse detection using gate-level characterization," in *Proceedings of the 46th Annual Design Automation Conference*. ACM, 2009, pp. 688–693.

[3] K. Xiao, D. Forte, Y. Jin, R. Karri, S. Bhunia, and M. Tehranipoor, "Hardware trojans: Lessons learned after one decade of research," *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, vol. 22, no. 1, p. 6, 2016.

[4] H. Salmani and M. Tehranipoor, "Layout-aware switching activity localization to enhance hardware trojan detection," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 1, pp. 76–87, 2011.

[5] B. Zhou, W. Zhang, S. Thambipillai, and J. Teo, "A low cost acceleration method for hardware trojan detection based on fan-out cone analysis," in *Proceedings of the 2014 International Conference on Hardware/Software Codesign and System Synthesis*. ACM, 2014, p. 28.

[6] K. Vaidyanathan, B. P. Das, E. Sumbul, R. Liu, and L. Pileggi, "Building trusted ics using split fabrication," in *2014 IEEE international symposium on hardware-oriented security and trust (HOST)*. IEEE, 2014, pp. 1–6.

[7] Z. Zhou, U. Guin, and V. D. Agrawal, "Modeling and test generation for combinational hardware trojans," in *VLSI Test Symposium (VTS)*, 2018, pp. 1–6.

[8] Y. Liu, K. Huang, and Y. Makris, "Hardware trojan detection through golden chip-free statistical side-channel fingerprinting," in *Proceedings of the 51st Annual Design Automation Conference*. ACM, 2014, pp. 1–6.

[9] F. Stellari, P. Song, A. J. Weger, J. Culp, A. Herbert, and D. Pfeiffer, "Verification of untrusted chips using trusted layout and emission measurements," in *2014 IEEE international symposium on hardware-oriented security and trust (HOST)*. IEEE, 2014, pp. 19–24.

[10] P. Song, F. Stellari, D. Pfeiffer, J. Culp, A. Weger, A. Bonnoit, B. Wisnieff, and M. Taubenblatt, "Marvel—malicious alteration recognition and verification by emission of light," in *2011 IEEE International Symposium on Hardware-Oriented Security and Trust*. IEEE, 2011, pp. 117–121.

[11] T. Hoque, S. Narasimhan, X. Wang, S. Mal-Sarkar, and S. Bhunia, "Golden-free hardware trojan detection with high sensitivity under process noise," *Journal of Electronic Testing*, vol. 33, no. 1, pp. 107–124, 2017.

[12] J. Balasch, B. Gierlichs, and I. Verbauwhede, "Electromagnetic circuit fingerprints for hardware trojan detection," in *2015 IEEE International Symposium on Electromagnetic Compatibility (EMC)*. IEEE, 2015, pp. 246–251.

[13] H. Salmani, M. Tehranipoor, and R. Karri, "On design vulnerability analysis and trust benchmarks development," in *2013 IEEE 31st international conference on computer design (ICCD)*. IEEE, 2013, pp. 471–474.

[14] B. Shakya, T. He, H. Salmani, D. Forte, S. Bhunia, and M. Tehranipoor, "Benchmarking of hardware trojans and maliciously affected circuits," *Journal of Hardware and Systems Security*, vol. 1, no. 1, pp. 85–102, 2017.

[15] S. Bhunia, M. S. Hsiao, M. Banga, and S. Narasimhan, "Hardware trojan attacks: threat analysis and countermeasures," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1229–1247, 2014.

[16] H. Salmani, M. Tehranipoor, and J. Plusquellic, "A novel technique for improving hardware trojan detection and reducing trojan activation time," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 20, no. 1, pp. 112–125, 2011.

[17] K. Xiao and M. Tehranipoor, "Bisa: Built-in self-authentication for preventing hardware trojan insertion," in *2013 IEEE international symposium on hardware-oriented security and trust (HOST)*. IEEE, 2013, pp. 45–50.

[18] Y. Jin and Y. Makris, "Hardware trojan detection using path delay fingerprint," in *2008 IEEE International workshop on hardware-oriented security and trust*. IEEE, 2008, pp. 51–57.

[19] N. Vashistha, H. Lu, Q. S, M. Rahman, s. Haoting, D. L. Woodard, N. Asadizanjani, and M. Tehranipoor, "Trojan scanner: Detecting hardware trojans with rapid sem imaging combined with image processing and machine learning," in *44st International symposium for testing and failure analysis, ASM*, 2018, pp. 256–266.

[20] T. Sugawara, D. Suzuki, R. Fujii, S. Tawa, R. Hori, M. Shiozaki, and T. Fujino, "Reversing stealthy dopant-level circuits," *Journal of Cryptographic Engineering*, vol. 5, no. 2, pp. 85–94, 2015.

[21] F. Courbon, P. Loubet-Moundi, J. J. Fournier, and A. Tria, "A high efficiency hardware trojan detection technique based on fast sem imaging," in *Proceedings of the 2015 Design, Automation & Test in Europe Conference & Exhibition*. EDA Consortium, 2015, pp. 788–793.

[22] X. Wang, H. Salmani, M. Tehranipoor, and J. Plusquellic, "Hardware trojan detection and isolation using current integration and localized current analysis," in *2008 IEEE international symposium on defect and fault tolerance of VLSI systems*. IEEE, 2008, pp. 87–95.

[23] K. Sanchez, P. Perdu, K. Melendez, and T. Nakamura, "Comparison of cw electro optical probing and light emission techniques," in *Proceedings of the 39th International Symposium for Testing and Failure Analysis (ISTFA)*, 2013, pp. 329–335.

[24] L. I. Rudin, S. Osher, and E. Fatemi, "Nonlinear total variation based noise removal algorithms," *Physica D: nonlinear phenomena*, vol. 60, no. 1-4, pp. 259–268, 1992.

[25] L. Vincent, "Morphological grayscale reconstruction in image analysis: applications and efficient algorithms," *IEEE transactions on image processing*, vol. 2, no. 2, pp. 176–201, 1993.