Programmable EM Sensor Array for Golden-Model Free Run-time Trojan Detection and Localization

Hanqiu Wang
ECE Department, University of Florida
Gainesville, FL 32611 USA
wanghanqiu@ufl.edu

Max Panoff
ECE Department, University of Florida
Gainesville, FL 32611 USA
m.panoff@ufl.edu

Zihao Zhan
ECE Department, University of Florida
Gainesville, FL 32611 USA
zhan.zihao@ufl.edu

Shuo Wang
ECE Department, University of Florida
Gainesville, FL 32611 USA
shuo.wang@ece.ufl.edu

Christophe Bobda
ECE Department, University of Florida
Gainesville, FL 32611 USA
cbobda@ece.ufl.edu

Domenic Forte
ECE Department, University of Florida
Gainesville, FL 32611 USA
dforte@ece.ufl.edu

***Abstract*—Side-channel analysis has been proven effective at detecting hardware Trojans in integrated circuits (ICs). However, most detection techniques rely on large external probes and antennas for data collection and require a long measurement time to detect Trojans. Such limitations make these techniques impractical for run-time deployment and ineffective in detecting small Trojans with subtle side-channel signatures. To overcome these challenges, we propose a Programmable Sensor Array (PSA) for run-time hardware Trojan detection, localization, and identification. PSA is a tampering-resilient integrated on-chip magnetic field sensor array that can be re-programmed to change the sensors' shape, size, and location. Using PSA, EM side-channel measurement results collected from sensors at different locations on an IC can be analyzed to localize and identify the Trojan. The PSA has better performance than conventional external magnetic probes and state-of-the-art on-chip single-coil magnetic field sensors. We fabricated an AES-128 test chip with four AES Hardware Trojans. They were successfully detected, located, and identified with the proposed on-chip PSA within 10 milliseconds using our proposed cross-domain analysis.**

***Index Terms*—EM sensor, side-channel, Hardware Trojan**

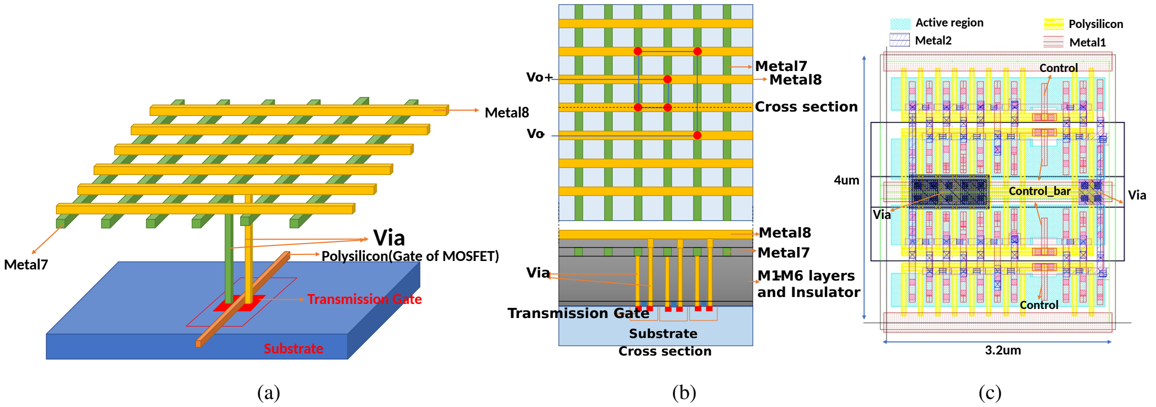
I. Introduction

Hardware Trojans (HTs) are malicious modifications inserted into ICs by adversaries during the fabrication or design process. These alterations can disrupt system functionality, causing security and privacy issues such as privacy leakage, denial-of-service and privilege escalation, etc. As the reliance on third-party designs and manufacturing continues to grow, the threat posed by HTs becomes more alarming. Over the years, researchers have discovered that HTs often produce detectable anomalies through side-channels like power consumption and electromagnetic (EM) emanations. The anomalies in side-channels can be detected after the chip is fabricated, either during the test phase or in run time, but often require costly external sensing setups and a golden model, a Trojan-free circuit used as a reference. This makes deploying some of these approaches in run time not applicable. Moreover, many side-channel oriented techniques suffer from low resolution of the collected traces.

As a result, on-chip sensors have gained attraction as a preferred solution. These sensors can intrinsically collect traces from EM side-channels through magnetic field coupling at run time with higher resolutions, thus ruling out the need for external measurement equipment (e.g., external probes, moving stages, etc.). Previous research by Jiaji et al. [1] used a single coil covering the entire chip area, which has low signal-to-noise ratio (SNR) issues. Consequently, this approach couldn't detect small HTs with few gates and required over 10,000 measurements to detect larger HTs. Its long mean time to detect (MTTD) limits its practical effectiveness.

In this paper, we propose a Programmable Sensor Array (PSA) to address the limitations of Jiaji's work. Our improved design, shown in Figure 1a, consists of a crossbar-like structure. The PSA can be programmed to different sizes and shapes, allowing it to cover or uncover specific parts of the chip for better SNR and HT localization. At each crossing point in the wire grid, a transmission gate (T-gate) controls the node's connectivity. This allows the sensor array to have different shapes, locations, and sizes. The size of a single sensor within the PSA can also be programmed to approximately match the size of a HT, ensuring the highest magnetic field emanations from HTs are captured. The improved SNR of PSA enables almost instant runtime detection, reducing MTTD significantly. The contributions of this paper can be summarized as follows:

- A novel on-chip PSA for EM side-channel measurement with big advantages over existing techniques was proposed, developed and validated.
- A silicon demonstration of the proposed PSA to detect and localize active HTs on an AES design implemented with TSMC 65nm technology.
- Significant SNR improvements with the proposed PSA compared to prior work.
- Experimental validation of the PSA's capability to detect, locate, and identify digital HTs within 10 ms with the proposed novel cross-domain analysis technique.



(a) (b) (c)

Fig. 1: (a)3D structure of on-chip PSA where top-level metals form the coils and transmission gate switches in the active layer control the size and shape at each intersection. (Only one MOSFET is shown for simplicity) (b)An example of PSA topology forming a 2-turn coil. The red dots denote the locations where switches are on. (c)T-gate layout.

II. Threat Model and Prior Work

A. Run-time Verification Versus Test-phase Verification

The distinction between run-time and test-phase verifications hinges primarily on the approach to HT detection. During the test phase, efforts are concentrated on the detection of HTs that can be intentionally triggered. The effectiveness of HT detection is evaluated based on the accuracy of feature and trace categorizations as well as the number of attempts needed to activate the Trojan. Most research focuses on developing algorithms to successfully trigger HTs within the minimum amount of time [2] [3]. Conversely, during run time, potential adversaries must first activate an HT before it can be detected if the whole batch of ICs is infected with HT, which is also the assumption of this paper. The primary metric is the duration between the Trojan's activation and its detection. This encompasses recognizing the system's activation and discerning the triggering conditions, often referred to as the Mean Time to Detect (MTTD) [4].

To reduce the hardware overhead during the evaluations, lightweight measurement and data processing components should be used. Bai et al. developed RASCv2 board, a compact 2cm x 2cm board that can replace an oscilloscope for side-channel analysis to detect malware [5] [6]. The board consists of two analog-to-digital converters (ADCs) for sampling EM and power side-channel traces, an EM antenna for signal capture, and an FPGA for data processing. The data processed by the FPGA are monitored by a security house via an onboard Bluetooth module, making run-time side-channel verification feasible. In this paper, we will integrate the concept of employing the RASC board (manufactured at a trusted facility) for data processing with the PSA's on-chip measurement capabilities to detect HTs in a real-time and trusted manner.

B. EM Side-channel Data Collection Methods

There are several existing techniques to detect and analyze EM side-channel leakage. Traditionally, external EM probes and oscilloscopes are used to collect EM side-channel emanation traces over IC packages. The captured signals will be analyzed in either the time or frequency domains to identify HTs [7]–[9]. To improve the quality of the collected traces and reduce overhead, He et al. introduced a single-winding on-chip EM sensor covering the whole chip to replace external probes [1]. In [9], Nguyen *et al.* introduced an EM backscattering-based Trojan detection approach. A transmitter antenna injects carrier signals into the IC, and the reflection signals that have been modulated with the activities of HTs are subsequently captured with a receiver antenna to identify HTs. This technique can detect impedance variations resulting from HT activities, even if these HTs have very small current consumption. Compared with our proposed PSA detailed in Section III, existing measurement techniques have problems of low SNR, limited spatial resolution, complex implementations, etc. These issues result in the limitations of HT detection rates, HT localization, and runtime deployment. A comprehensive comparison will be presented in Section III-B.

III. Programmable Sensor Array (PSA)

One of the main challenges of on-chip EM sensors is the balance among sensing area, accuracy, and cost. A single large sensing coil covering the entire chip is relatively easy to design and implement; however, it could be inaccurate due to magnetic flux self-cancellation[1]. Multiple smaller coils on the same layer may improve the overall resolution but would have smaller signal magnitudes and coverage. Using coils across multiplemetal layers can avoid these issues, but with extra cost. To mitigate these problems, we propose the PSA technique that enables the customization of sensor size and position on the chip at run time.

A. PSA Topology and Structure

PSA utilizes a wire grid that spans two metal layers, with a switch positioned at every intersection. Each switch is essentially a transmission gate (T-gate), depicted in Figure 1c, comprising a single PMOS and NMOS gate connected in

[1] Magnetic flux forming a small loop within a large sensor induces no voltage on it.

parallel. The shape, size, and location of a sensing array can be programmed at run time by controlling specific switches, as shown in Figure 1b. The size and location of PSA can be programmed via T-gates by connecting or disconnecting different cross-points on the wire grid or lattice. The lattice, comprising several rectangular sensing regions, can be used as part of the sensing array within the PSA.

Adjusting the shape and size of the PSA enables the PSA to circumvent the self-cancellation issue highlighted in [1], with many advantages. For instance, it facilitates the localization of any detected HTs by reshaping the sensing array. It also eliminates sensing boundary limitations or the need for significant overlap when employing multiple coils.

Implementing such side-channel sensors on chip will raise concerns on PSA's ability to execute side-channel attacks (SCA). Indeed, PSA itself does not protect from SCAs. But if adversaries can physically access the chip and conduct SCAs, it may be vulnerable to SCA regardless of the presence of PSA. Additionally, raw EM traces are not transmitted over any communication channels. Only processed data should be sent, and this can help prevent SCAs.

B. PSA Comparison with Prior Work

To highlight the improvement of the PSA-based HT detection technique over prior works, we made a comprehensive comparison in Table I. This comparison considers five criteria: HT detection accuracy, spatial resolution of the measurement, required number of traces, SNR, and feasibility for run-time deployment.

The approaches relying on traces collected from conventional external probes [7], [8] and on-chip single coils [1] fail to detect small HT with few gates (implemented as T3 in our chip in Table II). While Nguyen et al. [9] reports a 100% detection rate, their approach shares a common limitation with others: the inability to pinpoint the exact location of the HT on the chip. On the other hand, our PSA approach not only ensures a 100% detection rate but also stands out with the enhanced spatial resolution, providing the distinct capability of precisely identifying the HTs' physical location.

Due to low SNR, prior works often rely on statistical analysis, requiring numerous measurements to detect Trojans. For instance, Xiaolong et al. [7] and Jiaji et al. [1] compare the Euclidean distance between traces or explore the Euclidean distance distributions. Nguyen et al. [9] use Principal Component Analysis and K-means algorithm to categorize the collected spectra. These approaches require 100 to more than 10,000 measurements. In contrast, the EM side-channel traces from PSA exhibit sufficiently high SNR with an apparent difference between HT-inactive and HT-active traces. Therefore, fewer than ten measurements are needed, leading to a significantly shorter MTTD and faster Trojan detection.

For implementation complexity, unlike prior works necessitating cumbersome measurement devices [7]–[9], the PSA approach does not need external probes so it has high feasibility for run-time deployment. Fujimoto et al. also exploited the on-chip power noise measurement(OCM) to execute Correlational Power Analysis with high SNR [10], [11], it is also possible to use such OCM to detect HT, but that requires further investigation.

TABLE I: Comparison of EM side-channel data collection methods.

Features	**External Probe [7], [8]**	**Nguyen [9]**	**On-chip Single Coil [1]**	**PSA (proposed)**
HT Detection rate	Low	High	Low	High
HT Localization	No	No	No	Yes
Measurement#	>10,000	100	>10,000	<10
SNR	14.3dB	N/A	30.5dB	41.0dB
Run-time analysis	No	No	Yes	Yes

IV. PSA's Tamper-resilience

Hardware Trojan risk primarily originates from Third Party Intellectual Property (3PIP) vendors and malicious foundries. Our PSA approach is tampering-resilient and can effectively reduce the risks under both attacking scenarios. The effectiveness of PSA in detecting and locating HTs will be proved with the experimental results of Subsection VI-D. This section introduces a few case studies demonstrating PSA's resistance to tampering from either source.

A. Case 1: Malicious 3PIP

For malicious 3PIP attacks, as PSA is implemented on the two topmost metal layers after synthesizing the Register Transfer Level (RTL) code and is isolated from the main circuit, it would not interact with any 3PIP. Therefore, any pre-silicon modifications, including all potential 3PIP attacks, made prior to the layout phase will not compromise the PSA.

B. Case 2: Malicious Foundries

When dealing with malicious foundries, the PSA itself may be modified. However, tampering with such a mixed digital and analog structure is challenging. The adversary must modify additional circuitry, increasing the attack's complexity, thus lowering the attack's success rate. Additionally, any modifications that disable the PSA will trigger alarms during the test phase, as the PSA will return testing values.

Even if the attacker successfully completes the modifications, designers can easily detect them by reverse-engineering the two topmost metal layers. They are typically the thickest metal layers and are relatively easy to be reverse-engineered. Alternatively, designers can outsource the fabrication of the two topmost metal layers to other trusted foundries, a split-manufacturing method similar to those discussed in [12]. This provides an additional layer of security, making the PSA a robust defense against HT attacks.

V. PSA implementation on A Test Chip

A. Integrating PSA on AES-128 Test Chip

To assess the performance of PSA in both test and run-time phases we implemented and fabricated the PSA on the two top metal layers of an Advanced Encryption Standard (AES128) encryption design using TSMC65nm technology.

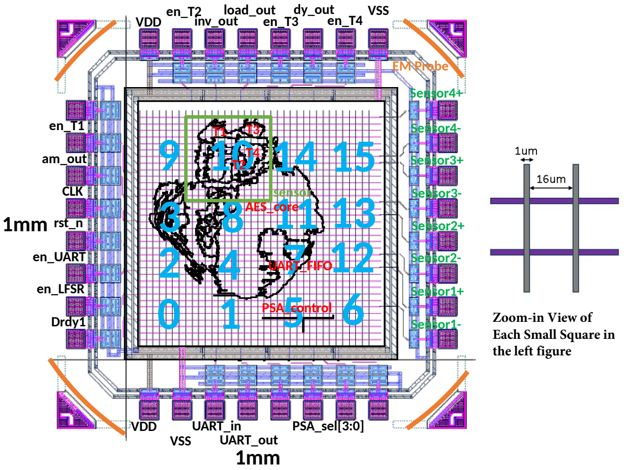


Fig. 2: Sensor deployment, IO pin assignment, and Amoeba module view on the AES128 test chip.

The proposed PSA was situated on layers Metal 7 and Metal 8 of the chip, covering the entire chip. It is a lattice including 36 horizontal wires, 36 vertical wires, and 1296 switches. The lattice wire measures 16μm in length and 1μm in width. Frequency sweeping is used to determine the optimal length and width that maximize the signal magnitude in the desired frequency range of 10MHz-100MHz.

For this test chip, the entire area was uniformly divided into 16 square sensing areas or sensors. Each sensor shares 33% of its area with adjacent sensors to ensure adequate circuitry sampling near the borders between any two sensors.

Main Circuit The underlying main circuit is an AES-128-LUT core, integrated with an RS232 UART communication module [13]. The clock frequency was set to 33MHz. The layout of the routing wires of the test chip, along with the indices of the PSA sensors, is illustrated in Figure 2.

HT Design The design incorporates four distinct HTs, modified from Trust-Hub [14] [15]. T1 is an amplitude modulation radio carrier Trojan capable of emitting an electromagnetic (EM) wave at a frequency of 750KHz. T2 is a chain of inverters connected to a key wire to amplify its leakage current. If T2 is implanted, attackers could recover the key via power analysis. T3 is a Code Division Multiple Access (CDMA) channel Trojan designed to leak the key, and T4 is a simple denial-of-service Trojan that elevates power consumption, potentially causing the IC to overheat. The four Trojans employ digital standard cells and each has unique triggering conditions. The 4 HT's locations are shown in the Amoeba view in Figure 2.

IO Pin Assignment The test chip uses a QFN 6mm x 6mm package and has 8 IO pins on each side. The IO pins' names are shown in Figure 2. The PSA uses the 8 IO pins on the right side. 2 IO pins are needed to measure the induced differential output voltage of one sensor, so we have 4 output channels, from sensor1+/- to sensor4+/-. The 4 sensors on each row use the channel on the same row. For example, sensor 0,1,5,6 in the figure uses sensor1 channel. The PSA control signals use 4 of 8 IO pins on the bottom side. They were decoded into gate signals for T-gates with the fully combinational decoder in the figure.

TABLE II: TROJAN GATES COUNT AND PERCENTAGE

Circuit	Overall	T1	T2	T3	T4
Standard Cell Number	28806	1881	2132	329	2181
Percentage	100	6.52	7.40	1.14	7.57

HT Triggering Condition T1 is activated periodically when a counter reaches 21'h1F_FFFF under the 33MHz clock. T2 is triggered when the first four bytes of the plaintext are 16'hAAAA. T3 and T4 are the always-on HTs, and we added external enable signals as triggers in experiments. The gate number counts and area ratios of these four HTs are shown in Table II.

We assess the performance of the PSA in detecting and locating HTs by activating and deactivating sensors during the execution of AES encryption. As depicted in Figure 2, the green box represents the area of a 6-turn-coil sensor, where most HT circuits are implemented. The orange arcs represent the size of a circle-shape external EM probe. The main circuit primarily falls under sensors 2, 3, 4, 7, 8, 9, 10, 11, and 14. Of these sensors, sensor 10 offers the most coverage of both Trojan payloads and triggers.

B. *T-gate Design and PSA Implementation Cost*

Due to the absence of the T-gates that fulfill our requirements in the standard cell library, we designed our own customized T-gates, which are illustrated within a 3.2μm x 4μm customized cell layout in Figure 1c. A single finger of the NMOS and PMOS devices in the design exhibit an aspect ratio of 500nm/60nm and 610nm/60nm respectively to have a similar current conducting capability. For enhanced performance, each of these MOSFETs incorporates 10 fingers. To ensure a low turn-on resistance, the layout features two PMOS and two NMOS devices, effectively creating a pair of T-gates connected in parallel. As a result, this T-gate configuration achieves a resistance of approximately 34 Ohms.

For power overhead, the dynamic power consumption of PSA sensors is negligible and largely contributed by the leakage power from the transistors. Therefore, PSA's impact on the overall power profile is minimal.

For area and resource allocation, the T-gates used in PSA account for an additional 5% of the total chip area, with the PSA located on metal layers M7 and M8. Despite this, the design effectively preserves routing capacity by aligning PSA wires parallel to main circuit wires, reducing top-layer routing capacity by just 6.25%.

In contrast to Jiaji's single-coil structure [1], which utilizes 100% of the top layer's routing capacity, PSA proves to be more efficient.

VI. EVALUATION ON TEST CHIP

A. *Test and Data Collection Platform Setup*

The test chip was mounted on a PCB board with voltage-level shifters and open-loop OP-AMPs. The output of each output channel of the PSA is amplified by a THS4504D

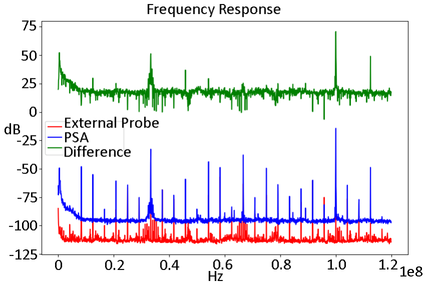


Fig. 3: Spectrum magnitude comparison between those from the PSA and an external EM probe.

OP-AMP with 50dB DC gain and 200MHz UGB, aligning well with our target frequency range from DC to 120MHz. A 33MHz crystal oscillator is used to generate the clock signal. The evaluation is conducted while the test chip executes AES-128 encryption. It receives plaintext from and sends ciphertext to a laptop through serial communications. During this operation, an oscilloscope or a spectrum analyzer triggered by the rising edge of the clock signal captures the amplified PSA output and generates the related frequency spectrum for further analysis. Additionally, we use the zero-span mode of the spectrum analyzer to measure the time-domain signal of the PSA's output at a desired single frequency.

For run-time deployment, a system integrated on the PCB board can replace the oscilloscopes, spectrum analyzers, and computers to measure and analyze side-channel data.

B. Signal-to-Noise Ratio (SNR) Measurement

To demonstrate the improved measurement quality offered by the PSA sensor array, we conducted SNR measurements and compared the results with those from an external Langer-EMV LF1 probe. We employ He's SNR measurement approach as detailed in [1]. Noise traces are first collected from the powered-up chip without any encryption activity. Signal traces are then gathered while the chip performs AES encryption. The SNR is calculated based on the root mean square (RMS) voltage ratio of these two data sets, as demonstrated in Equation (1).

$$SNR = 20log\left(\frac{Vrms_{signal}}{Vrms_{noise}}\right) \qquad (1)$$

The SNR of the PSA is 41.0 dB, surpassing both the external probe's 14.3 dB and the single-coil on-chip sensor's 30.5 dB as reported in [1]. In Figure 3, the green spectrum represents the difference in dB between the spectra from the sensor array and the external probe, demonstrating that the spectrum from the PSA can be up to 55 dB higher than that from an external EM probe. Overall, the proposed PSA structure offers significantly superior SNR results in comparison to either external probes or single-coil on-chip sensors.

The best state-of-the-art external probe is the ICR HH100-6 set with a diameter of 100 μm manufactured by the Langer EMV-Technik. Based on the manufacturers documents, the SNR of ICR probe is approximately 34dB below 120 MHz, so the best probe is still worse than our proposed PSA.

C. PSA Performance under Different Supply Voltages and Different Ambient Temperatures

We have conducted comprehensive evaluations of PSA's performance under varying operational conditions to confirm its suitability for runtime deployment across a wide range of applications. We performed simulations and experiments at different supply voltages, spanning from 0.8V to 1.2V, which covers the voltage supply voltage range for TSMC 65nm chips. Additionally, we carried out simulations under different ambient temperatures, ranging from $-40\,^{\circ}\mathrm{C}$ to $125\,^{\circ}\mathrm{C}$.

1) Voltage: Theoretically, a supply voltage increase results in a reduction of the turn-on resistance of T-gates. In the Virtuoso simulation, there was only a 4dB drop in the impedance of a single PSA sensor when the voltage supply was raised from 0.8V to 1.2V. We also made an experiment to measure the current response of the PSA by adding a 70mV frequency sweeping chirp signal to one sensor of the PSA and varying the supply voltage from 0.8V to 1.25V. The current does not change significantly, which agrees with the simulation results.

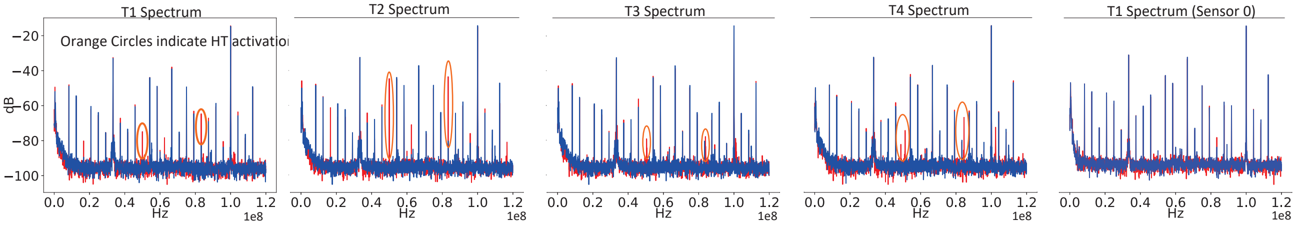
2) Temperature: Theoretically, an ambient temperature change only slightly affects the impedance of the PSA. Our simulations demonstrate that the impedance remains relatively stable, fluctuating within a range of 4dB.

D. Runtime Cross-Domain Analysis

For each of the 16 sensors, EM traces are recorded under five scenarios: when HTs T1, T2, T3, and T4 are individually activated and in the absence of any active HT. For always-on HTs, we use external enable signals to activate them. Each trace spans a frequency band from DC to 120MHz, populated with 2000 sample points. We averaged five collected traces to derive the spectrum shown in Figure 4. Notably, when examining the output from Sensor 10, as shown in Figure 4a, 4b, 4c, and 4d, two prominent frequency components at 48MHz and 84MHz, the sideband frequency components of the 1st and 3rd order clock harmonics, show up in the spectrum when HTs are active. We also record the traces from Sensor 0 as shown in Figure 4e, where no HTs are implemented beneath the sensor. There is hardly any spectrum difference that can distinguish HT's activities. This result further proves that our proposed PSA has the high spatial resolution needed to locate HTs.

In the experiments, we only need fewer than ten traces collected to detect a HT, resulting in less than 10 ms MTTD, a significant improvement over one single on-chip coil.

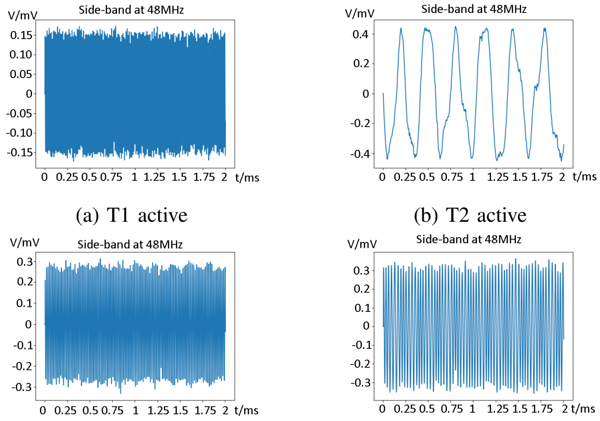
After identifying prominent frequency components related to HT's activities, we further switch back to the time domain by employing the zero-span mode of the spectrum analyzer to examine the time-domain waveforms of the two frequency components. Zero-span mode allows us to analyze the pattern of a time-domain signal at a desired fixed frequency. The time-domain waveforms at 48MHz when T1, T2, T3 and T4 are active are shown in Figure 5a, 5b, 5c, and 5d. It is shown that even if different Trojans leaked their information at the same frequency, the difference in their time-domain signals at 48MHz can still clearly differentiate different Trojans. This



(a) T1 active, Sensor 10 (b) T2 active, Sensor 10 (c) T3 active, Sensor 10 (d) T4 active, Sensor 10 (e) T1 active, Sensor 0

Fig. 4: Frequency response captured by sensors 10 and 0 for different HTs: red and blue colors represent the Trojan active and inactive cases, respectively.

is because different HTs result in different modulation patterns for clock frequency, and the information on modulation patterns is included in the time-domain waveforms of the side band frequency components. Therefore, by identifying the unique patterns in the time-domain signals, we can successfully classify all 4 HTs without full supervision.



(a) T1 active (b) T2 active

(c) T3 active (d) T4 active

Fig. 5: Time-domain signals of the identified prominent frequency components collected from the PSA sensor 10 were recovered with zero-span mode to differentiate different HTs successfully.

VII. Conclusion

In this paper, we proposed an integrated on-chip EM sensor array, PSA, that can be programmed to change its shape, size, and location. The PSA was implemented and tested in a 65nm technology node. The proposed PSA has a lower overhead than existing state-of-the-art on-chip coil sensor designs with much higher SNR and the capability of locating HTs. Furthermore, the MTTD during the runtime verification has been significantly reduced to less than 10 ms. The proposed cross-domain analysis can identify prominent frequency components that include the activity information of different Trojans in the frequency domain and differentiate different Trojans by examining the time-domain signals of these prominent frequency components by switching to the time domain.

VIII. Acknoledgement

This work was supported by the Office of Naval Research under Award Number N00014-19-1-2405.

References

[1] J. He, X. Guo, H. Ma, Y. Liu, Y. Zhao, and Y. Jin, "Runtime trust evaluation and hardware trojan detection using on-chip em sensors," in *2020 57th ACM/IEEE Design Automation Conference (DAC)*, 2020, pp. 1–6.

[2] R. S. Chakraborty, F. Wolff, S. Paul, C. Papachristou, and S. Bhunia, "Mero: A statistical approach for hardware trojan detection," in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2009, pp. 396–410.

[3] Y. Huang, S. Bhunia, and P. Mishra, "Mers: statistical test generation for side-channel analysis based trojan detection," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 2016, pp. 130–141.

[4] D. Forte, C. Bao, and A. Srivastava, "Temperature tracking: An innovative run-time approach for hardware trojan detection," in *2013 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, 2013, pp. 532–539.

[5] Y. Bai, A. Stern, J. Park, M. Tehranipoor, and D. Forte, "Rascv2: Enabling remote access to side-channels for mission critical and iot systems," *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, vol. 27, no. 6, pp. 1–25, 2022.

[6] Y. Bai, J. Park, M. Tehranipoor, and D. Forte, "Real-time instruction-level verification of remote iot/cps devices via side channels," *Discover Internet of Things*, vol. 2, no. 1, p. 1, 2022.

[7] J. He, Y. Zhao, X. Guo, and Y. Jin, "Hardware trojan detection through chip-free electromagnetic side-channel statistical analysis," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 25, no. 10, pp. 2939–2948, 2017.

[8] S. Faezi, R. Yasaei, and M. A. Al Faruque, "Htnet: Transfer learning for golden chip-free hardware trojan detection," in *2021 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, 2021, pp. 1484–1489.

[9] L. N. Nguyen, B. B. Yilmaz, M. Prvulovic, and A. Zajic, "A novel golden-chip-free clustering technique using backscattering side channel for hardware trojan detection," in *2020 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, 2020, pp. 1–12.

[10] D. Fujimoto, M. Nagata, S. Bhasin, and J.-L. Danger, "A novel methodology for testing hardware security and trust exploiting on-chip power noise measurement," in *The 20th Asia and South Pacific Design Automation Conference*, 2015, pp. 749–754.

[11] D. Fujimoto, N. Miura, M. Nagata, Y. Hayashi, N. Homma, Y. Hori, T. Katashita, K. Sakiyama, T.-H. Le, J. Bringer, P. Bazargan-Sabet, and J.-L. Danger, "On-chip power noise measurements of cryptographic vlsi circuits and interpretation for side-channel analysis," in *2013 International Symposium on Electromagnetic Compatibility*, 2013, pp. 405–410.

[12] J. Rajendran, O. Sinanoglu, and R. Karri, "Is split manufacturing secure?" in *2013 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, 2013, pp. 1259–1264.

[13] S. Morioka and A. Satoh, "An optimized s-box circuit architecture for low power aes design," in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2002, pp. 172–186.

[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] 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)*, 2013, pp. 471–474.