Runtime Trust Evaluation and Hardware Trojan Detection Using On-Chip EM Sensors

Jiaji He*, Xiaolong Guo†, Haocheng Ma‡, Yanjiang Liu‡, Yiqiang Zhao‡, and Yier Jin§
*Institute of Microelectronics, Tsinghua University, ‡School of Microelectronics, Tianjin University
Department of Electrical and Computer Engineering,†Kansas State University, §University of Florida
jiaji_he@mail.tsinghua.edu.cn, guoxiaolong@ufl.edu, hc_ma@tju.edu.cn, yanjiang_liu@tju.edu.cn, yq_zhao@tju.edu.cn, yier.jin@ece.ufl.edu

***Abstract*—It has been widely demonstrated that the utilization of post-deployment trust evaluation approaches, such as side-channel measurements, along with statistical analysis methods is effective for detecting hardware Trojans in fabricated integrated circuits (ICs). However, more sophisticated Trojans proposed recently invalidate these methods with stealthy triggers and very-low side-channel signatures. Upon these challenges, in this paper, we propose an electromagnetic (EM) side-channel based post-fabrication trust evaluation framework which monitors EM radiations at runtime. The key component of the runtime trust evaluation framework is an on-chip EM sensor which can constantly measure and collect EM side-channel information of the target circuit. The simulation results validate the capability of the proposed framework in detecting stealthy hardware Trojans. Further, we fabricate an AES circuit protected by the proposed trust evaluation framework along with four different types of hardware Trojans. The measurements on the fabricated chips prove two key findings. First, the on-chip EM sensor can achieve a higher signal to noise ratio (SNR) and thus facilitate a better Trojan detection accuracy. Second, the trust evaluation framework can help detect different hardware Trojans at runtime.**

I. Introduction

The rapid growth of the semiconductor industries results in a high demand of intellectual property (IP) suppliers, fabrication foundries, testing facilities, and further leads to the globalization of the IC supply chain. How to secure the entire IC supply chain becomes an extremely difficult challenge. Among all security threats, Hardware Trojans (HTs), the malicious modifications made to the integrated circuit (IC), are a promptly rising problem to the industry. Various hardware Trojan attacks and countermeasures have been intensely studied recently. The arms-race continues as more sophisticated Trojans and their countermeasures have been developed at all stages in the IC design flow.

Among all existing countermeasures, functional testing which uses modern EDA tools were first proposed but they can hardly detect the latest hardware Trojans [1], [2]. Side-channel based Trojan detection is one of the most convincing solutions to ensure the IC trustworthiness. Existing side-channel approaches follow the same pathway, where physical manifestations of the circuits are collected and analyzed to find the differences compared with trusted references. Based on global power consumption [3], path delays [4], currents on power grid [5], side-channel measurements and fingerprints can differentiate HT-inserted chips from genuine chips. However, attackers evade those approaches by designing hardware Trojans that are dormant at test time and are only activated later in the field of operation. More powerful and concealed Trojans were also developed recently. They are small enough to evade power consumption based fingerprinting detection methods and still are sophisticated enough to cause erroneous results or leak internal information [6], [7].Besides digital properties, analog properties are leveraged for HT designs where A2 [8] is a leading example. Analog Trojans break the digital assumption in previous hardware Trojan detection and testing approaches and produce minimal overhead in physical layouts.

In the meantime, previous on-chip structure based Trojan detection methods generally utilize specific functional structures, including time-digital-convector (TDC) [9] and ring-oscillator (RO) [10], to monitor the physical differences introduced by Trojans. Special on-chip structures were also proposed to monitor the logical differences by using the shadow register structure when the Trojan is activated [11]. These on-chip structures share a common problem of low coverage rates, where some vital abnormal behaviors caused by Trojans may not be detected. All previously developed on-chip Trojan detection structures also require significant modifications to the original design, which will cause undesired area and power overhead. Further, the insertion and integration of on-chip structures requires detailed understanding of the function of the original circuits, which makes the technique not easily be adopted as an add-on methodology.

To address all the above challenges and to evaluate trustworthiness of IC at the post-deployment stage, we propose a new framework to monitor the execution of circuits at runtime[1]. An on-chip EM sensor is involved in the framework which only relies on the modifications of the top metal layer of the original design and can be easily integrated into the IC design flow. After deployment (see Figure 1), the on-chip sensor measures EM radiations from circuit and then delivers the measurements to the data analysis module. Trust evaluation results would be provided from the analysis module to help identify malicious actions or vulnerabilities in the circuit. The main contributions of this paper are as follows:

- We propose a lightweight post-deployment framework for evaluating the vulnerability of the chip during the hardware execution. The framework can detect abnormal behaviors at runtime.
- As the key component of the framework, we present a method to design an on-chip EM sensor which is simple to deploy inside the chip. The proposed sensor is proven to achieve higher level of signal to noise ratio (SNR) compared to external EM probes.
- We validate the effectiveness of the proposed framework by fabricating a security-enhanced AES design along with four different types of hardware Trojans as a proof of concept.

The rest of the paper is organized as follows: In Section II, we introduce the attack model. We give a brief introduction on relevant background and explain our runtime framework, the on-chip structure and the statistic analysis in Section III. Simulations are performed to validate the effectiveness of the proposed framework in Section IV. Section V further presents demonstrations of our approach by fabricating a security-enhanced AES design. Conclusions are drawn in Section VI.

†Xiaolong Guo is the corresponding author.

[1]We define the runtime as the period when the system is running. It is different from real-time which responds immediately without any delay.

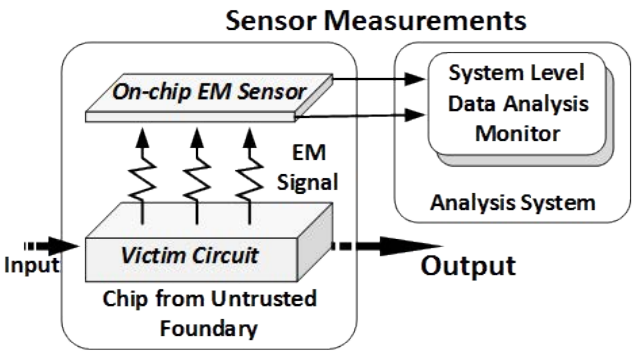


Figure 1: Deployment of the proposed trust framework.

II. Attack Model

We assume that hardware Trojans are of various types and can be embedded into different locations in the target circuit. Adversaries may exist among all of the stages in the hardware supply chain before the chip deployment. Once triggered, the inserted malicious logic may result in payloads such as deny of service (DoS), information leakage, functionality alterations, etc. The abnormal behaviors will inevitably cause abnormal currents within the circuit, thus contributing to EM radiation variations. Our framework targets all malicious Trojans which may draw abnormal current and cause different EM radiation patterns.In our attack model, we do not expect a trusted foundry but we assume that the analysis module running in collecting the EM measurement and processing the data is trusted. This module can be performed either in hardware, e.g., a programmable logic, an FPGA, or a dedicated ASIC, or in software[2]. To deploy the on-chip EM sensor, the only modifications made to the original design is to avoid any placement and routing on the top metal layer of the chip.

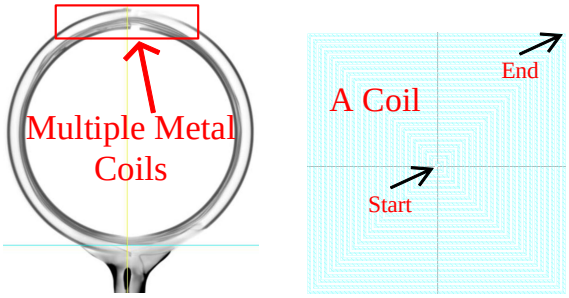
III. Post-deployment Trust Framework

A. EM Side-Channel based Trojan Detection Approaches

Among all side-channel parameters, EM is the most promising one and has many advantages over other side-channel parameters, including non-contact detection, location awareness, and rich in information [12]. However, the EM measurement setup usually requires specialized equipment which is often complicated and is difficult to achieve runtime trust evaluation. Besides, the measurement SNRis usually low especially when the EM radiation is collected by external probes. For those victim circuits deployed in an untouchable scenario such as cloud servers or distributed devices, it may be impractical to monitor circuit side-channel parameters using external probes.

To increase SNR, EM probes are often carefully designed. When researchers started to exploit EM radiation side-channel a couple decades ago, they usually designed a metal coil to collect the EM radiation [13]. Commercial EM probes are later developed such as the probes from LANGER [14] which are utilized in the EM radiation collection process. The signal intensity of direct EM radiation is closely related to the distance between the chip and the probe. Therefore, the hardware Trojan detection will be more accurate and sensitive via an on-chip EM radiation measurement. [15] designed an on-chip EM probe for collecting the EM radiation. Even though the EM probe is fabricated on a test chip using 150 nm technology, the on-chip probe is still far from the main circuit.

[2]The design details of this module is out of the scope of this paper. We use a trusted software module as an example in the paper for demonstration purpose.



(a) (b)

Figure 2: Probe structures of (a) one LANGER RF EM probe; (b) the designed on-chip EM sensor.

B. Post-deployment Trojan Detection Framework

The stealthy Trojan designs make the Trojan detection task more challenging and invalidate many of the previously proposed Trojan detection methods [8]. However, existing results also show that for any specific chip, if the EM traces for Trojans can be collected, the existence of hardware Trojans can be easily identified [12]. Therefore, post-deployment trustworthiness evaluation methods are more effective than pre-deployment stage solutions.

To enhance the post-deployment trust evaluation structure and to overcome the shortages within the existing Trojan detection method, we propose a new runtime trust evaluation framework which continuously monitors the circuit status and triggers an alarm once detecting Trojans or attacks from the analysis result. The proposed framework works in parallel with the circuit's normal execution hence there is no runtime performance degradation. Figure 1 shows the structure and deployment of the newly proposed runtime trust evaluation framework. The new framework performs the runtime trust evaluation and achieves high detection capability by adding an EM sensor on the chip and a data analysis system module off-chip. The basic working procedure of the proposed runtime Trojan detection framework is straightforward. In order to increase the accuracy of the EM radiation measurements, the EM sensor is deployed at the top metal layer of the same die. The total EM radiation of the circuit is measured by the on-chip EM sensor. The measured EM signal traces will then be sent to the data analysis module.

In the data analysis system, the EM signal traces will be processed following regular side-channel fingerprinting methods. We assume the users know how the circuit will operate, thus the features of the circuit's EM side-channel can be defined through simulations. If the inserted Trojan is activated, the Trojan's EM radiation would introduce extra and abnormal features different from the pre-defined circuit features of the EM side-channel, thus an alarm signal will be triggered for further investigations.

C. On-Chip EM Sensor Design and Deployment

The external EM probe is usually composed by several metal coils with the same diameter at the top end of the probe to help gather EM radiations. We scan a LANGER RF EM probe in an X-ray machine and the structure of the probe is demonstrated in Figure 2(a). Some, though minor, optimizations are performed on the EM sensor to adapt to the ASIC structural features. The overall structure of on-chip sensor is similar to the external EM probe. That is, the proposed on-chip EM sensor is designed as a coil starting from the center, extending to the corner and covering the entire circuit. The structure is demonstrated in Figure 2(b). The overall EM sensor structure is simple enough that any tampering of the sensor can be

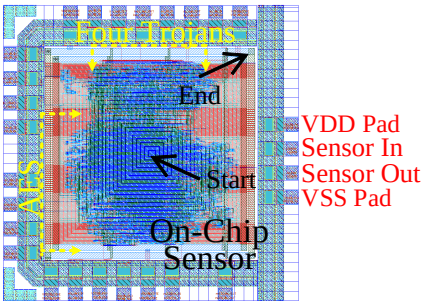


Figure 3: Layout of the circuits with on-chip sensor integrated.

easily identified through basic measurements. In order to obtain the best EM radiation collection results, the width of the coils in this paper is set not to violate the design rules of the minimum width of the wires defined in the technology library.

Modern CMOS manufacturing techniques utilize substrate to build the transistors and multiple metal layers for local and global wiring and connections. There are two types of metal layers in the circuits, namely the lower metal layers utilized to form connections within and between standard cells and the higher metal layers to route the power/ground wires. The designed EM sensor will be placed at the topmost metal layer in the chip in our trust framework. The cost of fabricating and deployment of the proposed EM on-chip sensor can then be reduced significantly. Further, the utilization of the topmost metal layer can explore the EM leakage of the whole circuit at runtime. The one-way spiral coil structure also improves the perception of EM signal detection. The sensitivity of the EM sensor highly depends on the magnetic flux passing to the coil so the effectiveness of the detection using the proposed EM sensor equals to the accumulation of all the coils with gradually increasing diameters. Considering that the sensor is inside the chip, a high SNR value can be achieved during measurements. With the increasing of the perception and sensitivity, more comprehensive and accurate information can be obtained from the measured EM radiation signals.

D. Trojan Detection Algorithm

To achieve the goal of Trojan detection, the data analysis module in this framework is also important. As shown in Figure 1, it leverages various data analysis algorithms which we will discuss in this section. The monitor keeps reading the EM sensor output in the format of voltages. Different from previous on-chip trust framework [7], we design the module as a software program which performs sophisticated data analysis algorithms without adding computation burdens on the chip. Software level code verification may be used to ensure the integrity and trustworthiness of the program.

The hardware Trojans will introduce extra side-channel abnormal behaviors either in the triggering process or when the Trojans are activated. The EM side-channel information generally has more interference than other side-channel parameters. Techniques such as Principal Component Analysis (PCA) can help reduce the dimensionality of original data by replacing several correlated variables with a new set of independent variables.

Note that the goal of Trojan detection algorithms is to detect the abnormal features introduced by the inserted Trojans. Euclidean distance is an effective similarity metric to measure the differences among the data sets. The Euclidean distances among the possible Trojan-infected and Trojan-free design are determined. The hardware Trojan can be identified when the differences exceed the threshold value. The threshold value is defined to be the maximum Euclidean distance (D_{th}) among the data of Trojan-free design, which is described as Equation (1) where D_g is the data sets of Trojan-free design. D_i and D_j are the i_{th} and j_{th} sample of D_g, respectively. The threshold is set in order to handle the unintended noise and other influence factors that still exist after the denoising and principle analyzing process [12].

$$ED_{th} = \underset{D_i, D_j \in D_g}{argmax} \|D_i - D_j\|^2 \quad (1)$$

Table I: Trojan sizes compared to the whole AES design

Circuit	AES	T1	T2	T3	T4	A2
Gate Count	33083	1657	2793	250	2793	N/A†
Percentage	100%	5.01%	8.44%	0.76%	8.44%	0.087%‡

† Not applicable.
‡ Calculated based on circuit area.

E. Analog Trojan Vulnerability Detection

Besides detecting the Trojans utilizing the traditional algorithms, we also target detecting analog Trojans, such as A2 Trojan [8], which invalidates the traditional side-channel detection methods. In order to leverage the on-chip sensor, the data collected by the on-chip sensor is processed in the frequency domain to identify the abnormal fast flipping Trojan trigger signals. Normally, the circuits underneath the on-chip sensor will generate specific EM spectrum, which will concentrate around the operating frequency of the circuits accompanying certain harmonic frequency. When the A2-style Trojans are being triggered, the fast flipping signals will result in extra frequency spots or increased amplitude in the spectrum. Although previous methods that target the detection of the A2-style Trojans can detect the Trojans by monitoring specific signal wires, these methods suffer from the problem of low coverage rate [16]. The on-chip sensor, on the contrary, overcomes this problem as the entire chip is covered by the sensor with high resolutions. The spectrum inspection of the EM radiation enables the detection of tiny abnormal features.

IV. Simulation Results of the Framework

To demonstrate the effectiveness of the proposed trust evaluation framework, a simulation model is developed based on the layout of an AES encryption design, four digital hardware Trojans and one A2-style analog Trojan. Three simulation experiments are carried out to validate the feasibility and effectiveness of the developed framework.

A. Simulation Setup

We develop the four Trojans modifying benchmarks from TrustHub [17], and designs of the Trojans are introduced as follows. Trojan 1 leaks the secret information through the AM radio carrier at a 750 KHz frequency and the leaked information can be demodulated with a wireless radio receiver. Trojan 2 leaks the secret information through the leakage current which is generated by one shift register and two inverters. When the lower bit of the shift register is “0”, within a pre-set time, a leakage current will be generated between the PMOS of the first inverter and the NMOS of the second inverter. Trojan 3 leaks the secret information through a Code Division Multiple Access (CDMA) channel which utilizes multiple clock cycles to leak a single bit. A pseudo-random number generator is used to provide a CDMA sequence for the exclusive OR operation on the secret information. Trojan 4 causes performance degradation of the circuit. It increases the power consumption by introducing more flipping registers after activation. An A2-style Trojan is also simulated with only six CMOS transistors. The trigger input, which needs to be a digital pulse signal, is provided by the on-chip clock

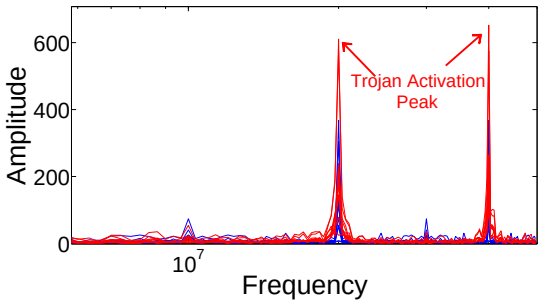


Figure 4: A2 Trojan detection in frequency domain.

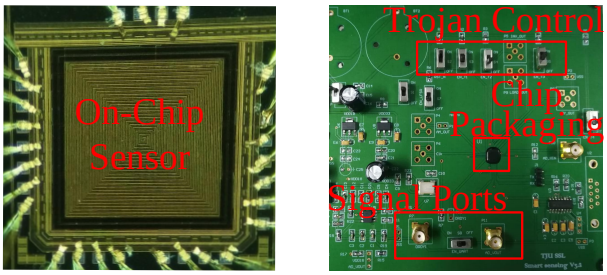


Figure 5: Die image of the fabricated AES (left) and the customized PCB with chip-on-board packaging (right).

division signal. The area of the Trojans compared with the original circuit are shown in Table I.

The layout-level EM simulation method in [18] is applied. We first performed transistor-level circuit simulations to obtain transient current sets in Hspice. Then these current sets are appended to corresponding resistive elements to form the IC's current distribution network, in which the physical information of these resistive elements is obtained from the extracted parasitic file. Finally, EM radiation computation is performed and EM leakage from every point of the IC's surface can be acquired. We also build simulation models of the external probe and on-chip sensor based on their structures. According to Faraday's law, induced electromotive force (emf) of these probes are calculated for EM radiation evaluation.

B. On-chip Sensor Feature Simulation

The on-chip sensor has many advantages over an external probe. The most significant one is that the on-chip sensor can maintain a higher SNR than the external probe. Thus it is easier for the on-chip sensor to collect more EM signals generated by stealthy Trojans, such as A2 Trojans. The external probe is inevitable to be disturbed by environmental noises in collecting EM radiations, while the proposed on-chip EM sensor is less affected.

To quantitatively demonstrate the effectiveness of the internal on-chip sensor, an EM model is constructed as the EM radiation source. Then the on-chip sensor and external probe are added to the model to collect the simulated radiation. Random white noise is also added in the simulation to mimic the real-world environment noises. The external probe is set 100 μm above the circuit, and the parameter is set with reference to the real thickness of packaging of the chip. The simulated EM radiation in voltage and root mean square (RMS) voltage, $SNR_{voltage}$, is calculated by utilizing the obtained voltage data as shown in Equation (2).

$$SNR_{voltage} = \frac{Signal_{VoltageRMS}}{Noise_{VoltageRMS}} \tag{2}$$

In this equation, as the environmental noise of the circuit is added, the SNR can be calculated using Equation (3).

$$SNR_{dB} = 20log_{10}(SNR_{voltage}) \tag{3}$$

The SNR simulation results from the on-chip sensor is 29.976 dB, while the SNR simulation results from the external probe is 17.483 dB. Apparently, by using the on-chip sensor, we obtain much higher SNR for the radiation signal.

C. Hardware Trojans Detection Simulation

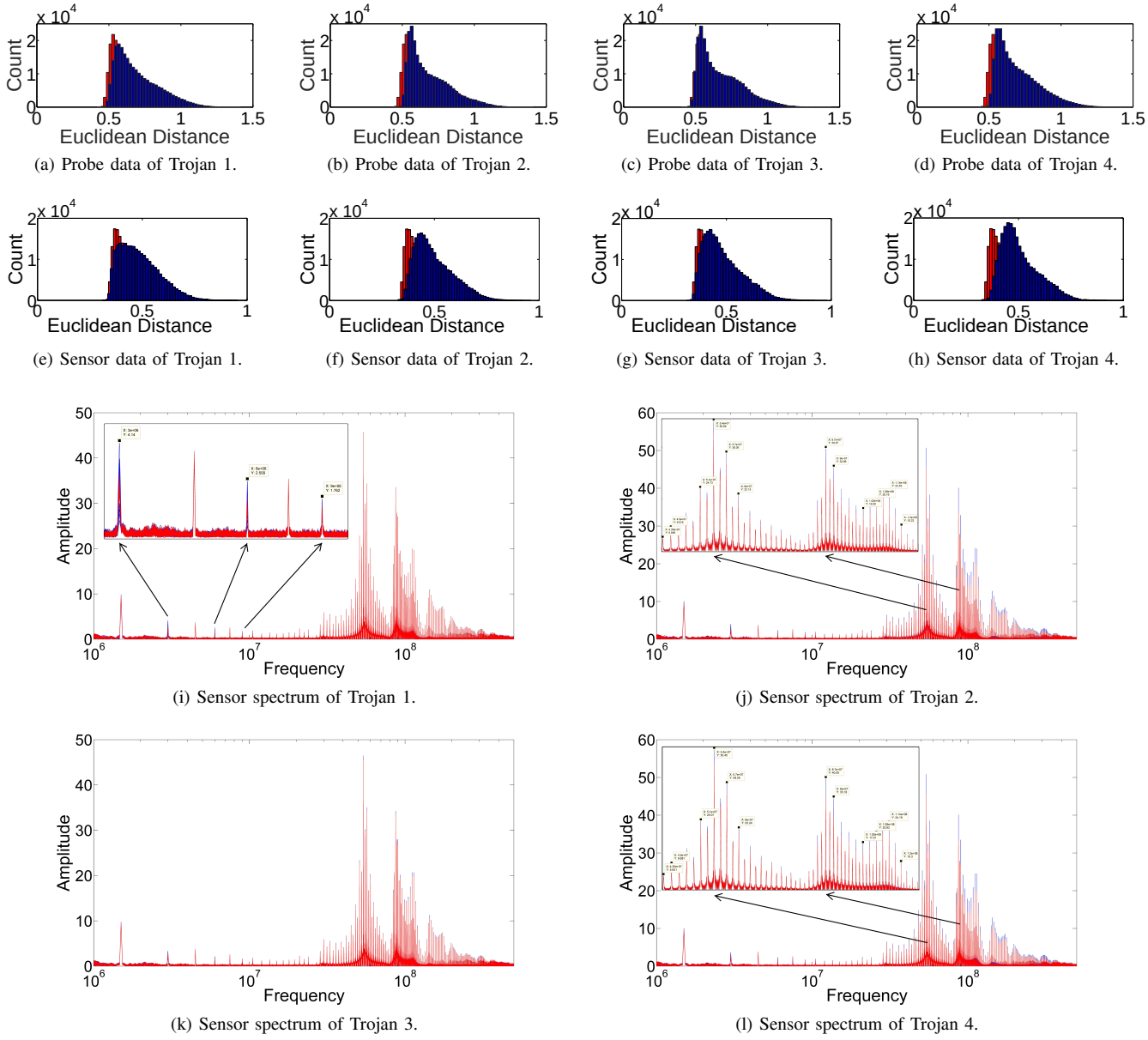
In order to demonstrate the on-chip sensor's capability in detecting digital hardware Trojans, a 128-bit AES is implemented utilizing 180 nm CMOS technology with four different hardware Trojans inserted into the circuit. Besides the original triggering mechanism, we design an extra triggering signal for each Trojan to activate the payload in a more manageable way. The EM on-chip sensor is designed utilizing the topmost metal layer in 180 nm CMOS technology, i.e., the sixth metal layer (M6) of the layout. The AES circuit together with four different Trojan circuits are implemented utilizing the metal layer one to five (M1 to M5). A model of the AES circuits and four Trojans is constructed based on the layout illustrated in Figure 3, and the EM radiation collected by the on-chip sensor is also simulated. There are four pads for the on-chip sensor: power supply *VDD* pad, ground connection *VSS* pad, *Sensor In* pad that connects the start point of the sensor and *Sensor Out* pad that connects the end point of the sensor. The output signal of the on-chip sensor will be the voltage differences between the start point and end point of the coil.

During the simulation process, we firstly collected the measurements from the on-chip sensor when there are no Trojans being activated, and the simulated EM radiation serves as the reference in the Trojan detection. We then trigger each Trojan in turn and measures the corresponding simulated EM radiation. After all the data being collected, the Euclidean distances are calculated using the algorithm described in Section III-D. The Euclidean distances between the reference circuit and Trojan 1, 2, 3, and 4 circuits are 0.27, 0.25, 0.05, and 0.28, respectively. Those distances are highly distinguishable in the scenario of simulations. Overall, all four traditional Trojans are detected by the on-chip sensor.

D. Analog Trojan Detection Simulation

The newly proposed analog Trojan utilizes a fast toggling signal for Trojan activation which introduces extra spectral components in the frequency domain. The Trojan can be detected by checking the distribution of spectrum spots in the acquired EM traces. We denote the original circuit's frequency as g and the signal transition frequency introduced by the HT as T. If the signal transition frequency T coincides with a frequency spot of the original circuit g (such as the clock signal, i.e., $T = g$), then we can determine whether a hardware Trojan has been inserted into the chip by comparing the magnitude of frequency spot g. If T does not coincide with clock signal, i.e., $T \neq g$, we treat the influence of the hardware Trojan as a newly added frequency spot. By analyzing the aforementioned formulae, we can decide the existence of the hardware Trojan by the comparison of the magnitudes at the frequency spots. During the comparison process, Fast Fourier Transform (FFT) will be performed to transform the EM traces to frequency domain in order to reveal more information concerning the frequency spots and their corresponding magnitudes.

After transferring the simulated EM radiation into the frequency domain, the EM spectra are compared to check whether there are any abnormal fast toggling signals beyond the normal operation range. The simulation results are demonstrated in Figure 4. The red lines are the spectrum when the A2-style Trojan is in the triggering state, while



(a) Probe data of Trojan 1. (b) Probe data of Trojan 2. (c) Probe data of Trojan 3. (d) Probe data of Trojan 4.

(e) Sensor data of Trojan 1. (f) Sensor data of Trojan 2. (g) Sensor data of Trojan 3. (h) Sensor data of Trojan 4.

(i) Sensor spectrum of Trojan 1. (j) Sensor spectrum of Trojan 2.

(k) Sensor spectrum of Trojan 3. (l) Sensor spectrum of Trojan 4.

Figure 6: Trojan detection results with external probe (top row), on-chip sensor (middle row) and sensor spectrum (bottom row).

the blue lines are the original circuit performing the same operation. The first peak on the left is the clock signal and the second peak on the right is the second doubled harmonic of the clock signal. As clearly demonstrated in the frequency spectra, the A2-style Trojan introduces a higher amplitude in the spectra. In the simulation setup, the Trojan trigger is provided by the on-chip clock division signal. The Trojan's activation alters the original distribution of the EM spectra and the Trojan activation peak is illustrated in the figure.

V. Experimentation on Fabricated Chip

Besides simulation results presented in Section IV, we fabricated the AES encryption circuit along with four hardware Trojans utilizing the 180 nm CMOS technology. A customized PCB board is designed specifically to validate the on-chip EM sensor and the trust evaluation framework. The die image of the fabricated chip and the PCB board are shown in Figure 5. In this section, we demonstrate the effectiveness of the proposed framework by analyzing the EM radiations in terms of Euclidean distances and spectral features.

A. Measurement Accuracy of On-chip EM Sensor

In the experiments, the signals from the external probe and on-chip sensor is collected simultaneously. In real-world measurement, it is very difficult to access to the clear signals without any noises. Therefore, we measure the signal and noise separately within the same environment by collecting the voltage data using an oscilloscope. Specifically, in the first step, the chip is powered up without executing the encryption, and the collected signal is considered as environment noises. In the second step, the chip starts executing the encryption operation. Therefore, the collected signals include the EM radiation from the encryption operation and noises. The SNR is calculated according to the equations in Section IV-B. The measured SNR of the on-chip EM sensor output is 30.5489 dB, while the SNR of the external probe output is 13.8684 dB. Compared with the

simulation SNR results, the SNR of the external probe is lower than the simulation results because there are more unintended influences. Still, the experimental results clearly validate the effectiveness and superiority of the proposed on-chip sensor in detecting EM signals.

B. On-chip Hardware Trojans Detection

The two output signals of the on-chip sensor are treated as a differential signal pair and the voltage difference is the on-chip sensor's output. The Trojans are activated in sequence and the EM radiations from the external probe and on-chip sensor are collected. Utilizing the Trojan detection algorithm presented in Section III-D, the Trojan detection results are illustrated in Figure 6. From Figures 6(a) to 6(d), we show the Euclidean distances of Trojans' EM radiations measured by the external probe. The red stripes imply the circuit's EM radiation without Trojan activation, and the blue stripes illustrate the Trojan activated circuit's EM radiation data. Overall, all the Trojan activated stripes are not separated with the original circuit's data. Note that the two EM radiations in Figure 6(c) are almost completely overlapped, as the Trojan 3 has the smallest area overhead. Euclidean distances from the rest of 3 figures are also overlapped and in the same trend with the area overhead in Table I. Note that the peaks of distributions of original circuit and Trojan activated circuit are not separable. As a result, it is quite challenging for the probe to distinguish the Trojans from the original circuit without further data analysis methods.

Figures 6(e) to 6(h) demonstrate the Euclidean distances of the on-chip sensor collected Trojans' EM radiations. As a result, all the Trojans are detected. From the distributions of the results, the body of the original circuit's data is still largely overlapped with the body of the Trojan activated circuit's data. However, because the on-chip sensor has a higher SNR compared with the external probe, the peaks of distributions of the original circuit and Trojan activated circuit are separable. The Trojan detection results in Figure 6(f) and 6(h) illustrate an obvious improvement by using the sensor. Thus if the original circuit's EM radiation distributions are pre-defined, the Trojans can be detected if the shifting of the distributions' peaks are observed runtime. For the Trojan 1 detection results, the distribution of the on-chip has a flat peak which is quite different from the original circuit's distribution. The Trojan 1 can be detected through feature analysis of the data because the distribution changes distinctly. The separation of the distribution peaks in the Figure 6(g) demonstrate that the Trojan 3 is detected by using the sensor. Overall, the Trojan distinguishability of the on-chip sensor is better than external probe.

On the other hand, because of the high SNR and on-chip structure, the proposed sensor is capable for analyzing spectral features of the EM radiations. All the Trojans are detected efficiently except the Trojan 3. The collected sensor data of four Trojans are obtained through FFT, and the results are illustrated in Figures 6(i) to 6(l). The red lines in the spectrum illustrate the original circuit's EM data, and the blue lines illustrate the Trojan activated circuits' EM data. As illustrated in Figure 6(i), the Trojan 1 introduces extra energy at a lower frequency range and the zoomed part is also demonstrated. From Figure 6(j) and 6(l), the Trojans introduce significant amplitude increase in a number of frequency spots. The overall energy peaks for Trojan 4 are higher than that for Trojan 2, and this observation correspond to the results shown in Figures 6(f) and 6(h). The reason for the similar distributions is that both Trojan 2 and 4 utilize more registers. As to the Figure 6(k), the frequency spots are not distinguished clearly because of the extreme low overhead of the Trojan 3. Another reason is that we only perform the analysis on the raw data from on-chip sensor directly.

VI. Conclusion and Future Work

In this paper, we developed a runtime trust evaluation framework based on an on-chip EM sensor. The on-chip sensor has advantages over the external probe by achieving a higher detection accuracy and a flexible deployment. In the future, we will fabricate A2-style analog Trojans to further validate the effectiveness of the propsed framework. The structure of the on-chip EM sensor will also be enhanced to increase the SNR of the measured EM signals.

Acknowledgments

This work was partially supported by Office of Naval Research (ONR) Young Investigator Program (YIP) and AFRL CYAN Center of Excellence. Dr. Jiaji He was supported in part by the China Postdoctoral Science Foundation under Grant 2019TQ0167.

References

[1] Y. Jin, N. Kupp, and Y. Makris, "Experiences in hardware trojan design and implementation," in *2009 IEEE International Workshop on Hardware-Oriented Security and Trust*. IEEE, 2009, pp. 50–57.

[2] 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.

[3] D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi, and B. Sunar, "Trojan detection using ic fingerprinting," in *2007 IEEE Symposium on Security and Privacy (SP'07)*. IEEE, 2007, pp. 296–310.

[4] Y. Jin and Y. Makris, "Hardware Trojan detection using path delay fingerprint," in *IEEE International Workshop on Hardware-Oriented Security and Trust*, 2008, pp. 51–57.

[5] R. Rad, J. Plusquellic, and M. Tehranipoor, "Sensitivity analysis to hardware Trojans using power supply transient signals," in *HOST*, 2008, pp. 3–7.

[6] Y. Jin, D. Maliuk, and Y. Makris, "Post-deployment trust evaluation in wireless cryptographic ics," in *Proceedings of the Conference on Design, Automation and Test in Europe*. EDA Consortium, 2012, pp. 965–970.

[7] Y. Jin and D. Sullivan, "Real-time trust evaluation in integrated circuits," in *2014 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE, 2014, pp. 1–6.

[8] K. Yang, M. Hicks, Q. Dong, T. Austin, and D. Sylvester, "A2: Analog malicious hardware," in *2016 IEEE symposium on security and privacy (SP)*. IEEE, 2016, pp. 18–37.

[9] D. Ismari, J. Plusquellic, C. Lamech, S. Bhunia, and F. Saqib, "On detecting delay anomalies introduced by hardware trojans," in *International Conference on Computer-aided Design*, 2016.

[10] X. Zhang and M. Tehranipoor, "Ron: An on-chip ring oscillator network for hardware trojan detection," in *Design, Automation & Test in Europe*, 2011.

[11] L. Jie and J. Lach, "At-speed delay characterization for ic authentication and trojan horse detection," in *IEEE International Workshop on Hardware-oriented Security & Trust*, 2008.

[12] 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.

[13] J.-J. Quisquater and D. Samyde, "Electromagnetic analysis (ema): Measures and counter-measures for smart cards," in *E-smart*, 2001.

[14] LANGER, *https://www.langer-emv.com/en/index*.

[15] M. Yamaguchi, H. Toriduka, S. Kobayashi, T. Sugawara, N. Hommaa, A. Satoh, and T. Aoki, "Development of an on-chip micro shielded-loop probe to evaluate performance of magnetic film to protect a cryptographic lsi from electromagnetic analysis," in *2010 IEEE International Symposium on Electromagnetic Compatibility*, July 2010, pp. 103–108.

[16] Y. Hou, H. He, K. Shamsi, Y. Jin, D. Wu, and H. Wu, "R2d2: Runtime reassurance and detection of a2 trojan," in *2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, April 2018, pp. 195–200.

[17] Trust-HUB, *https://www.trust-hub.org/*.

[18] A. Kumar, C. Scarborough, A. Yilmaz, and M. Orshansky, "Efficient simulation of em side-channel attack resilience," in *2017 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, Nov 2017, pp. 123–130.