IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 25 September 2024, accepted 9 October 2024, date of publication 14 October 2024, date of current version 24 October 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3479929

SURVEY

A Survey of Electromagnetic Radiation Based Hardware Assurance and Reliability Monitoring Methods in Integrated Circuits

MANOJ YASASWI VUTUKURU, (Graduate Student Member, IEEE), JOHN M. EMMERT, (Senior Member, IEEE), AND RASHMI JHA, (Member, IEEE)
Department of Electrical and Computer Engineering, University of Cincinnati, Cincinnati, OH 45221, USA

Corresponding authors: Manoj Yasaswi Vutukuru (vutukumi@mail.uc.edu) and Rashmi Jha (jhari@ucmail.uc.edu)

This work was supported by NSF Center for Hardware and Embedded System Security and Trust (CHEST) Industry-University Cooperative Research Centers (IUCRC) under Grant NSF CNS 1916722.

ABSTRACT Electromagnetic (EM) radiation-based hardware assurance methods are gaining prominence due to their non-invasive nature of monitoring the chip activity and the potential for continuous monitoring of integrated circuits (ICs) during operation. This paper presents an in-depth survey on the existing EM-based strategies for detecting hardware Trojans, counterfeit components, and monitoring the reliability of ICs. The paper discusses diverse methods of capturing EM emissions, with traditional near-field probes and the emerging on-chip antenna structures, while discussing the benefits and challenges associated with each method for continuous ICs monitoring to improve their security and reliability. Furthermore, the survey provides a comprehensive summary of the experimental setups and analytical techniques employed in earlier works for enhancing the security and reliability of ICs. This survey paper advances our knowledge of EM-based hardware assurance techniques to monitor the reliability of ICs.

INDEX TERMS Aging, counterfeit detection, electromagnetic emissions, electromigration, hardware Trojan detection, on-chip EM sensor, reliability, side-channel analysis.

I. INTRODUCTION

Integrated Circuits (ICs) have become vital in modern day electronic systems with wide spectrum applications ranging from consumer electronics to critical sectors like military, aerospace, medical devices, smart grids, transportation, and data centers. To meet the tough time-to-market demands, the semiconductor supply chain has progressively become global, manufacturing components in different locations. However, globalization is inherently associated with multiple security vulnerabilities, potentially exposing ICs to risks like Trojan insertions and counterfeit components, which significantly compromises the reliability of ICs during operation.

Reports indicate a substantial increase in the entry of counterfeit electronic devices in the market, with their market share now in the billions of dollars [1], [2], [3], [4]. In the light of this, there has been an intensive effort to develop assurance methods for detecting hardware Trojans (HTs) [5], [6], counterfeit ICs, and reliability analysis [7], [8] to reinforce the security of ICs, Field Programmable Gate Arrays (FPGAs) and other electronic devices [9].

Although several methods are being developed to prevent counterfeit, recycled, and remarked ICs, there is always a chance for a motivated attacker to bypass these measures and compromise the system by HT insertion. Additionally, there are various device-level degradation processes like Bias Temperature Instability (BTI) [10], Hot Carrier Injection (HCI) [11], and Time-Dependent-Dielectric-Breakdown (TDDB) [12] which can cause aging and lead to device failure. Moreover, continuously switching HTs can accelerate this aging by increasing on-chip currents and temperature of a chip during operation [13].

Even in the emerging 2.5D/3D ICs, thermal management is a major issue which could impact the reliability of the chiplets [14]. Problems like electromigration, triggered by high current densities and elevated temperatures, can lead to defects in the chip interconnects, causing signal loss [15].

The associate editor coordinating the review of this manuscript and approving it for publication was Harikrishnan Ramiah.

Hence, there is a need to estimate the performance and reliability of ICs to ensure ideal device behavior during operation.

To address this, different methods were developed for aging detection by designing sensors to monitor the critical path delays of the circuit under test (CUT) during operation [16], [17], [18], [19], [20]. Other methods also employed aging sensors based on ring oscillators (ROs) and ferroelectric field-effect transistors (FeFETs) to predict aging [21], [22]. However, these sensors add area overhead and are challenging to implement in mission critical systems.

Having continuous monitoring techniques for integrity and reliability monitoring of ICs can enhance the security and trust of electronic systems. One interesting method involves monitoring the IC activity with unintentional electromagnetic (EM) emissions during its operation [23]. By capturing the EM traces and analyzing the activity of the CUT, we can get crucial information on the behavior of ICs. Several studies on EM side-channel analysis (EM-SCA) reported the extraction of cryptographic keys by capturing the EM traces from ICs and FPGAs [24], [25], [26].

While much of the EM-SCA research focuses on cryptographic key extraction, recent works have employed the EM traces for developing hardware assurance methods due to their non-destructive and contactless way of security and reliability monitoring. On-chip antennas are also being developed to capture the EM emissions to perform EMI measurement, HT detection, and prevent fault injection attacks [27], [28], [29]. These on-chip antennas provide better signal to noise ratio and spatial resolution over the conventional near-field probes due to their proximity to the chip surface [28]. Integrating such on-chip antennas to continuously monitor the EM emissions from the ICs for providing real-time reliability information would help the users monitor the remaining useful life of the system and prevent early failures.

In this paper, we survey the existing works related to EM-based hardware assurance techniques. EM-based approaches are highly versatile, capturing both digital and analog emissions to provide a more comprehensive view of a circuit's activity. These methods enable continuous monitoring during operation without interfering with the IC's functionality. Moreover, recent advancements in data processing, such as machine learning, have enhanced the capability of EM-based methods to analyze large datasets, making them effective in detecting malicious modifications and predicting long-term reliability. We categorize EM-based hardware assurances into three primary types: hardware Trojan (HT) detection, counterfeit detection through device fingerprinting, and reliability monitoring, demonstrating how unintentional EM emissions can be leveraged to enhance the security and reliability of ICs and electronic systems.

The paper is organized as follows: section II discusses fundamentals about factors such as aging and electromigration that affect the reliability of ICs. In section III, we discuss the role of near-field EM emissions in the domain of security and reliability from an adversarial and security perspective. Section IV outlines various measurement procedures of near-field EM emissions such as near-field probes and on-chip antenna structures. Section V provides a survey of various EM-based HT detection, counterfeit detection, and reliability monitoring methods. Section VI discusses some existing designs and challenges of fabricating and testing on-chip antennas for continuous IC activity monitoring during operation. Section VII focuses future research directions related to EM-based hardware assurance, finally concluding with section VIII.

II. BACKGROUND AND RELEVANT INFORMATION

A. AGING IN TRANSISTORS

Transistors age over time because of factors such as Bias Temperature Instability (BTI) [30], Hot Carrier Injection (HCI) [31], [32], and Time Dependent Dielectric Breakdown (TDDB) [33]. All these phenomena essentially increase the threshold voltage of the transistor and cause degradation of channel mobility, transconductance and drain current. This degradation of the device properties increases the delay in the critical path of the circuit and causes timing failures. BTI is of two types, Negative BTI (NBTI) and Positive BTI (PBTI) which occurs in PMOS and NMOS transistors respectively. In the older technology nodes, NBTI used to be a major challenge whereas PBTI was not observed. However, with the use of high-k dielectric materials in advanced technology nodes, PBTI was observed in NMOS devices too [34]. There are multiple works which attempt to explain the cause of BTI in transistors [35], [36], [37], [38]. The primary reason is the formation of traps in the gate oxide when the silicon-hydrogen bonds break near the interface due to the high electric fields and temperatures and diffuse towards the gate. There are two theories namely reaction-diffusion (RD) and trapping/de-trapping (TD) which explain the diffusion mechanism of BTI. A brief review on BTI and other degradation and aging models can be found in this paper [39].

Hot carrier degradation or injection (HCI) is also caused by trapped high energetic carriers in the gate oxide. The kinetic energy of the carriers increases when high electric fields are applied, and they are accelerated into the gate dielectric region causing degradation. There are four types of carrier injection mechanisms which can be found in this article [40]. Overall, BTI and HCI have similar effects on the MOS devices. However, reports have shown that BTI has some recovery phase whereas HCI has permanent effect on the device performance [41], [42]. Similarly, TDDB is a time-dependent degradation mechanism that depends on the dielectric material of the device. As higher electric fields are applied to the device, breakdown of the dielectric material occurs which damages the transistor (Fig. 2). Different types of breakdown mechanisms and the underlying physics can be found in [12], [43], and [44]. Accelerated aging of the device occurs if these degradation phenomena are accelerated by compromised fabrication or high operating temperatures which adversely affect the reliability of the system.

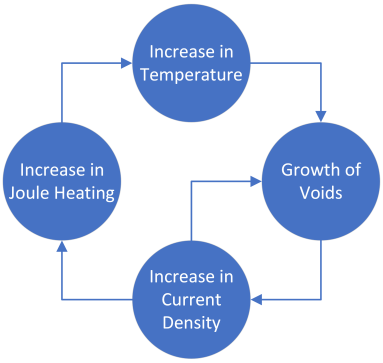

FIGURE 1. Joule heating and growth of voids in interconnects.

B. ELECTROMIGRATION IN INTEGRATED CIRCUITS

Electromigration is a form of interconnect aging predominantly seen in ICs and Printed Circuit Boards (PCBs). The metal interconnects are stressed because of high current densities and strong electric fields leading to short or open circuit failures [45], [46], [47]. When high currents flow through the metal interconnects, the metal-ions are diffused along the interconnect in the direction of the flow of electrons. This diffusion of ions which is characterized by ion flux density, is dependent on the magnitudes of two opposing forces. The forces which keep the ions in place (nature of conductor, crystal size, interface, and grain boundary chemistry) vs. the forces that try to dislodge the ions such as current density, temperature, and mechanical stress [48]. Asymmetry in the ion flow causes open-circuit failures called voids and short-circuit failures called hillocks in the interconnects (Fig. 2). The median-time-to-failure (MTTF) of an interconnect is explained by Black's equation

$$\text{MTTF} = A \times J^{-n} \times \exp\left(\frac{E_a}{k \times T}\right) \tag{1}$$

where A is a constant dependent on cross-section-area, J is the current density, n is a scaling factor (1 or 2), E_a is the activation energy for electromigration, k is the Boltzmann constant, and T is the temperature [49].

Joule Heating is another factor which affects the reliability of an IC. It is a self-heating process which occurs because of high current densities in the interconnects which eventually leads to electromigration [50], [51]. Fig. 1 shows the relation between temperature, void formation, current densities, and joule heating. As the temperature in the chip rises due to high current densities or compromised fabrication process, voids are formed due to electromigration and joule heating. Formation of voids causes less current to flow through the interconnects and ultimately cause signal loss or device failure impacting the reliability of the system. Joule heating and electromigration essentially increase the resistance of the interconnects as the current flow decreases because of the voids. This characteristic can be used to detect electromigration and monitor reliability of the circuit [52].

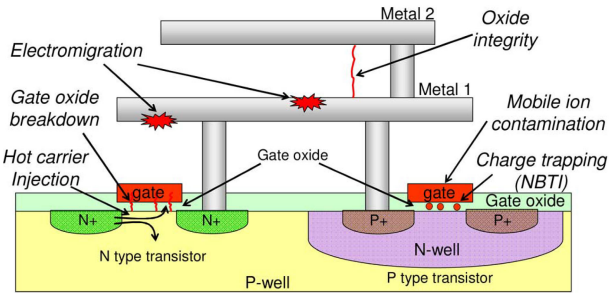

FIGURE 2. Failures in CMOS circuits (BTI, HCI, Electromigration) [53]

III. ROLE OF ELECTROMAGNETIC RADIATION IN HARDWARE ASSURANCE

Electromagnetic side-channels are a significant source of information leakage in ICs. As the circuit size decreases, density of the metal wires and other components increases leading to more EM emissions in the near-field [54]. This phenomenon occurs because the metal wires within the chip act as antennas, radiating EM waves when current flows through them. The EM emissions are said to be in the near-field when the distance, r is less than $0.1 \times \frac{\lambda}{2\pi}$ where λ is the wavelength of the EM signal [55].

The EM emissions from ICs, micro-controllers and FPGAs have been utilized to extract information about the underlying circuit in electronic systems [56]. These emissions consist of electric-field (E-field) and magnetic-field (H-field) components. H-field emissions are typically measured in the near-field because they are less affected by ambient noise and other materials compared to E-field emissions [57]. Near-field probes are commonly used to measure both H- and E-field emissions from an IC or a PCB [58]. While H-field measurements are made through contact less methods, the E-field probes need to be in contact with the surface of the IC. The proximity and precise positioning of the H-field probe relative to the surface of the IC are crucial for collecting high-quality EM traces [58].

In the case of hardware security, understanding the role of these unintentional EM emissions in analyzing the side-channel attacks or providing security is essential. Fig. 3 shows an overview of the role of near-field EM emissions in hardware security, trust and reliability of ICs and embedded systems. From an attackers perspective, these emissions can be exploited to conduct EM-SCA attacks to extract the crpytographic keys, perform EM-fault injection attacks to introduce system faults, and potentially cause EMC non-compliance. On the other hand, from a security standpoint, the same emissions can be utilized for security measures, including counterfeit detection through device fingerprinting, hardware Trojan (HT) detection, and reliability monitoring.

IV. MEASUREMENT OF NEAR-FIELD EM RADIATION

A. NEAR-FIELD EM PROBES

To extract information from EM emissions, it is essential to capture multiple signal traces while the device-under-test (DUT) is operating. Several leading manufacturers,

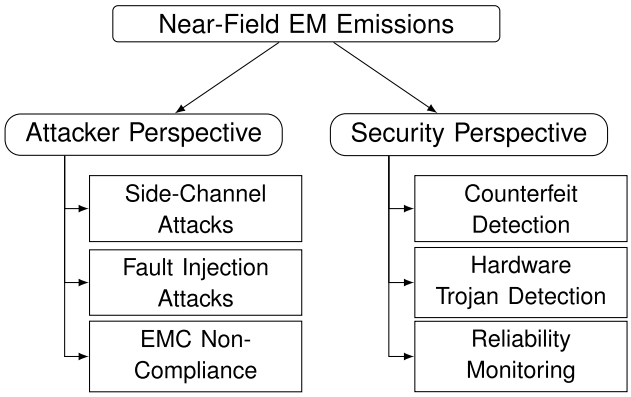

FIGURE 3. Overview of near-field EM emissions in hardware security.

including Langer EMV-Technik, Rohde & Schwarz, and TekBox, supply near-field probes designed to measure electromagnetic interference (EMI). Typically, these probes are employed to perform EM compliance checks, ensuring that there is no excessive leakage of EM radiation from ICs or other electronic devices [59]. Researchers have utilized these commercial probes in side-channel analysis to extract secret encryption keys from encryptions like AES and RSA [60], [61], and for security applications such as HT detection and counterfeit detection. In addition, some researchers developed custom E-field and H-field probes for sensing EM emissions from ICs [62], [63], [64], [65].

While these probes can be effectively used for off-chip monitoring of the EM emissions from an IC, there are some challenges with the probe measurements in real-world scenarios. Probes are highly sensitive to environmental noise, and the distance of the probe from the surface of the IC determines the quality of the data collected. To collect data over a longer period from different locations on the chip, automatic probe movement is required. Authors in [66] and [67] developed an algorithm to automatically scan the region of interest on the IC surface to collect high quality data. Although these methods are useful for off-chip EM side-channel monitoring, they are not suitable for providing security through continuous monitoring during runtime. To address this, recent research has focused on developing on-chip antenna structures or antenna arrays that can measure the EMI of an IC for real-time security applications [27], [28], [29].

B. ON-CHIP ANTENNA STRUCTURES

As an alternative to traditional near-field probes, on-chip antenna structures can be integrated directly onto the silicon substrate to capture EM emissions from a chip during its runtime. These on-chip antennas provide better signal to noise ratio as compared to traditional probes due to their proximity to the CUT. Common antennas like monopole, dipole, loop and Yagi-Uda are suitable for on-chip integration. In addition to these traditional designs, custom antenna configurations are often developed to meet specific system requirements.

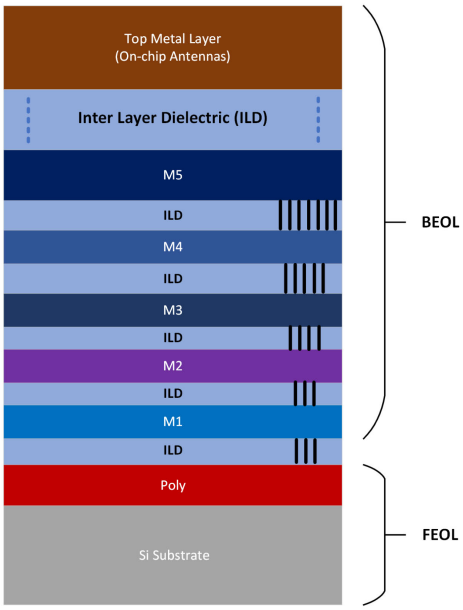

FIGURE 4. BEOL on-chip antenna fabrication stack [68] © 2024 IEEE.

For designing the on-chip antennas, it is essential to consider various parameters such as the resonant frequency (f_r), geometry, dimensions, and fabrication process. These antennas are predominantly used in high frequency applications like millimeter-wave (mm-wave) and terahertz (THz) wireless communications, where scaling down antenna size to achieve higher f_r is more feasible. However, since chips operate at lower frequencies, larger antennas are required to target lower resonant frequencies, as f_r is inversely proportional to the length (L), of the antenna ($f_r \propto \frac{1}{L}$). Miniaturization techniques are necessary to optimize antenna size and f_r to reduce area overhead during IC integration. A typical CMOS fabrication stack of on-chip antennas with several metal layers in the back end of the line (BEOL) is depicted in Fig 4. Here, the top metal layer can be used for fabricating and integrating the antennas at the BEOL. Different types of on-chip antennas employed for Trojan detection, and reliability monitoring are surveyed in section VI.

V. SURVEY OF EM-BASED HARDWARE ASSURANCE OF INTEGRATED CIRCUITS

The topics covered in the survey are broadly categorized into HT detection, counterfeit detection, and reliability monitoring of ICs and FPGAs. Counterfeit detection methods include different techniques for device identification, circuit activity identification, and IC authentication using EM-based fingerprinting. The papers were collected from databases like Google Scholar, IEEE, ACM, MDPI with focus on the hardware security applications mentioned above.

A. EM-BASED HARDWARE TROJAN DETECTION

HTs are malicious modifications made to ICs that can disrupt the ideal operation of a device or system. HTs can be

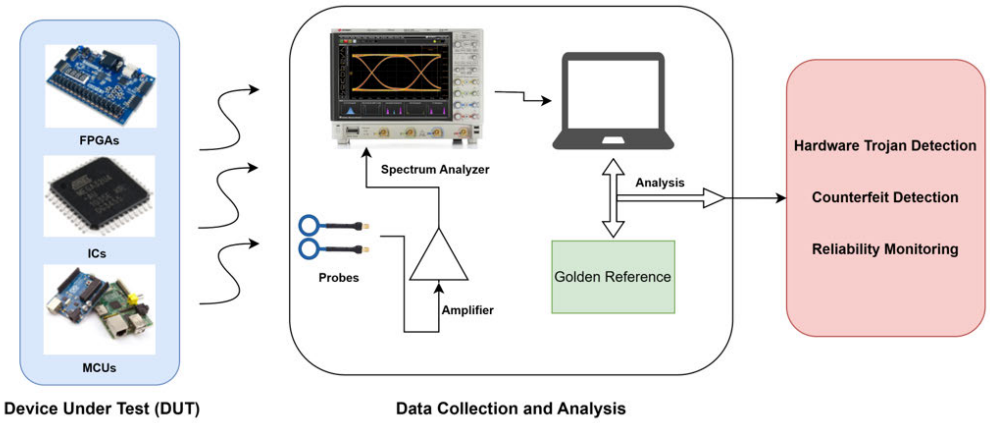

FIGURE 5. Overview of EM side-channel based hardware assurance methods.

classified into two main types: digital HTs and analog HTs. Digital HTs are designed to alter the operation of a circuit by modifying logic gates or flip-flops in the circuit, while analog HTs are designed to disrupt the operation of a circuit by introducing parasitic elements that can alter the circuit's performance. The detection of HTs is a challenging problem because they are designed to be stealthy and difficult to detect with normal testing methods. A broad overview on the emerging trends in HT detection can be found in [5], [69], and [70].

One of the first comprehensive surveys on HT classification and detection was compiled by Tehranipoor and Koushanfar [69]. The authors define HTs, provide a detailed taxonomy of their characteristics, and discuss the challenges of detecting these malicious modifications. The survey explores various detection methodologies, including side-channel analysis techniques like power and timing analysis, and Trojan activation strategies. Hayashi and Kawamura [70] discuss various detection methods, including side-channel information analysis, gate-level characteristic evaluation, test-based detection, optical inspection, formal verification, and electrical property measurement. They particularly highlight the possibility of HTs being implemented outside the IC itself, such as on peripheral circuits or wiring, and explain how these HTs can be used to leak information using EM waves. Recently, Liakos et al. [5] categorized HTs, examined their structure and attack mechanisms, and reviewed existing countermeasures, including side-channel analysis, logic testing, machine learning, and runtime monitoring. The paper discussed various machine learning models that could be employed in building ML-based frameworks for HT detection.

Among the various pre-silicon and post-silicon HT detection methods discussed in these surveys, side-channel based methods have been most widely used due to their advantages in terms of extracting information about the DUT. Power, timing, and EM are some of the prominent side-channels through which circuit information can be extracted. Power side channels analyze the power consumption patterns of a device, utilizing specialized setups to monitor current or voltage. This method requires physical access to the power supply lines and is highly sensitive to variations in power consumption and noise. Timing side channels exploit variations in the execution time of operations by measuring register-to-register path delays and comparing them with process variation delays. This approach is useful for detecting deviations caused by HTs in the circuit's timing behavior [69], [70]. Recently, EM-based methods have become popular for HT detection because they enable non-contact detection and localization, adding minimal overhead to the original circuit. Compared to power side channels, EM-based methods allow for non-invasive detection without requiring access to power lines and can capture emissions from specific regions of the chip, providing more localized information. In contrast to timing side channels, EM-based techniques offer more precise localization, are less sensitive to clock variations, and can capture both digital and analog activities, making them more versatile for detecting a wider range of HTs.

A typical process flow of EM side-channel based hardware assurance is shown in Fig. 5. EM traces are collected from the DUTs using near-field probes, which are connected to an amplifier and a spectrum analyzer. These collected traces are then analyzed and compared with a golden reference to detect HTs, counterfeit components and to monitor the reliability of the DUTs. In contrast to the papers discussed above, this section surveys works that exclusively focus on utilizing EM side-channel to provide security and assurance through HT detection using near-field probes.

One of the first works on EM-based HT detection was done by Söll et al. in 2014 [71]. They utilized an EM side-channel analysis technique for detecting HTs on FPGAs. Using a Xilinx Virtex-II Pro target platform, the study successfully distinguished malicious designs from genuine ones by comparing their EM emanations against a golden reference. The detection of HTs was found to be influenced by factors such as the Trojan's location and logic distribution. The experimental setup consisted of a Langer-LF B3

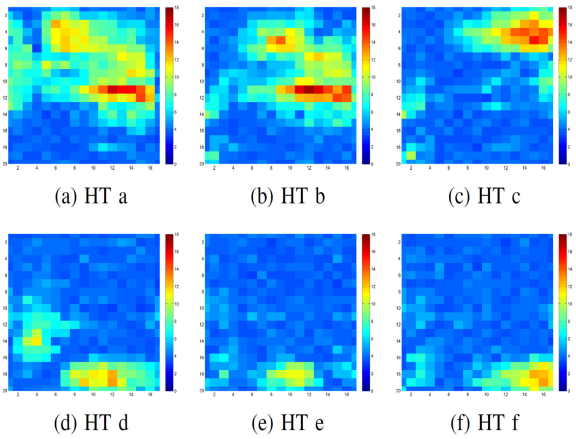

FIGURE 6. (a)-(f) Detection of HTs at different locations [72] © 2014 IEEE.

near-field probe and a LeCroy WavePro digital oscilloscope for data collection and analysis. This method demonstrated the detection and localization of HTs by calculating the absolute difference of all the measured EM traces. While this work successfully detected HTs based on EM emissions, the HT that was implemented was relatively big in size, which is not usually the case in real world scenarios.

To demonstrate the detection of extremely small Trojans, Balasch et al. [72] proposed an EM fingerprinting based method by implementing extremely small Trojan circuits at various locations on the FPGA. Using a SASEBO-G development board which houses two Virtex-II Pro FPGAs, the study successfully detected the presence of very small HTs (80-bit comparator) in an AES-128 implementation by comparing the Trojan-infected circuit with golden reference. In this, a Langer ICR HH 500-6 H-field probe was used to collect EM traces and the data was analyzed using Welch's two-tailed T-test for both the golden reference and the DUT. The resultant EM bitmap was compared for identifying and locating the tiny Hardware Trojans on the FPGA as shown in Fig. 6.

While the above two methods used EM emissions to successfully detect HTs, they needed golden reference ICs to compare the EM profiles of Trojan-infected circuits against. In real world, it is difficult and expensive to obtain a golden reference IC for EM measurements. To this end, He et al. [26] developed a novel golden chip-free methodology for HT detection, using EM side-channel statistical analysis. This method does not require golden chips for comparison against HT infected circuits. Instead, they simulate and model the EM spectrum of the original circuit from an RTL level circuit implementation on an FPGA. This simulation considers data transitions in the registers and look up tables (LUTs) to model the reference EM as seen in (2) where $R(t)$ is the simulated trace at moment of transition, t, D_i is the fan-out number of the i_{th} register or LUT, P_i and Q_i are initial and final states of i_{th} register or LUT and $\oplus$ is an XOR operator. V_m represents the number of input vectors which are used for modeling the EM trace. Using a SAKURA-G development board, around 11 AES-128 benchmarks obtained from TrustHub [73] were implemented to collect EM data with a Langer RF-R 50-1 probe. The authors compare simulated and measured EM spectra using the Euclidean distance metric, achieving 100% accuracy in detecting the HTs at different locations of the FPGA.

$$R(t) = \sum_{i=1}^{n} D_i \times (P_i \oplus Q_i)\Big|_{V_m} \tag{2}$$

Another approach by Liu et al. [74] utilized side-channel correlation analysis to detect the HTs. This method exploits correlations between transient current and EM emissions to identify the existence of Trojans, and utilizes a ring oscillator (RO) network for test vector generation. The ROs increased the Trojan switching activity in the CUT and correlation analysis was performed to extract the additional EM generated due to HT activation. TrustHub AES-128 benchmarks [73] were implemented using a SAKURA-G development board and the EM traces were collected using a Langer RF2 probe connected to an amplifier and a MSO4054 digital oscilloscope.

Research focused towards detecting firmware changes in FPGAs by using EM side-channel analysis was conducted by Fuller et al. [75]. The authors developed a method to detect changes as small as a single logic element being moved by one slice in the FPGA. The method can also identify whether HTs were injected into the bitstream, even if they remain dormant as the additional injected logic changed the EM emission profile of the FPGA. A CUT comprising of a serial communication core and an arithmetic algorithm was implemented on an Artix-7 FPGA. Incremental changes to the logic were made and EM traces were collected for 13 bitstreams. The EM emissions were analyzed by signal processing and machine learning techniques like Support Vector Machine (SVM) and Linear Discriminant Analysis (LDA) to classify the changes in the CUT with an accuracy of 100% for one device and 99.8% for 10 different devices of the same FPGA family.

Following the similar trend, Chen et al. [76] also developed EM-based HT detection method for FPGAs which are extensively used in IoT applications. The technique analyzes EM radiation of the FPGA's clock tree to detect the presence of HTs. The authors demonstrated the effectiveness of their method through various experiments and discussed the impact of experimental parameters such as step size, scanning area of the probe and the ambient temperature on the HT detection rate. The clock tree EM emissions were collected from two Artix-7 FPGAs by an EMP 340HS probe connected to a LeCroy oscilloscope. Trojan benchmarks on AES - 128 (AES-T100, AES-T200, and AES-T300) and RSA - 128 (BasicRSA-T200, BasicRSA-T400) from TrustHub [73] were used to program the FPGAs for analysis. The collected EM data was analyzed by using a back propagation neural network (BPNN) with accuracy of 100% for always-on HTs and 92% for triggered HTs.

TABLE 1. Summary of EM-based hardware trojan (HT) detection methods.

Authors	Assurance Method	Experimental Setup	Circuit Under Test (CUT)	Analysis Metrics
Söll *et al.* [71]	HT Detection	(1) Virtex-II FPGAs (2) Probe: Langer EMV (3) LeCroy Oscilloscope	CUT: AES Trojan: Sequential Trojans	Absolute difference
Balasch *et al.* [72]	HT Detection	(1) SASEBO-G: Virtex-II FPGAs (2) Probe: Langer ICR 500-6 (3) Digital Oscilloscope	CUT: AES-128, Trojan: 80-bit Comparator	Welsch's T-test
He *et al.* [26]	HT Detection	(1) SAKURA-G: Spartan-6 FPGAs (2) Probe: Langer RF-R 50-1 (3) Tektronix MSO4054	CUT: AES-128, Trojan: TrustHub Benchmarks	Euclidean Distance
Liu *et al.* [74]	HT Detection	(1) SAKURA-G: Spartan-6 FPGAs (2) Probe: Langer RF2 (3) Tektronix MSO4054 (4) LabVIEW	CUT: AES-128, ROs Trojan: TrustHub Benchmarks	Correlation Analysis
Fuller *et al.* [75]	HT Detection in FPGA Firmware	(1) Arty: Artix-7 FPGAs (2) Probe: Riscure RF (3) LeCroy SDA-813Zi-B (4) MATLAB	CUT: Serial Communication, Collatz Algorithm Trojan: Modfied CUT	SVM and LDA
Chen *et al.* [76]	HT Detection	(1) Artix-7 FPGAs (2) Probe: EMP 340HS (3) LeCroy WavePro 610Zi	CUT: AES-128 Trojan: TrustHub Benchmarks	PCA and BPNN
He *et al.* [28]	HT Detection using On-chip Sensor	(1) AES-128 Chip: 180 nm CMOS (2) On-Chip Sensor (3) Testing Platform	CUT: AES-128 Trojan: TrustHub Benchmarks A2-Style Analog HT	Euclidean Distance
Adibelli *et al.* [65]	HT Detection using Backscattered EM	(1) Cyclone-V FPGA (2) Probe: Custom E and H (3) Vector Network Analyzer	CUT: AES-128 Trojan: TrustHub Benchmarks	Frequency Domain Analysis
Chen *et al.* [81]	HT Detection using On-chip sensor	(1) MTJ Sensor (2) Fabrication Facility (3) Cadence (4) Verilog-A	CUT: Power Amplifiers Trojan: Custom HTs	Bayesian Neural Network
He *et al.* [77]	Chip-Free HT Detection	(1) SAKURA-G: Spartan FPGAs (2) Probe: Langer RF-R 50-1 (3) Tektronix MSO4054	CUT: AES-128, RSA-128 Trojan: TrustHub Benchmarks	K-Means Clustering
Zhang *et al.* [78], [79]	HT Detection	(1) Altera Cyclone FPGAs (2) Probe: RF Probe From [80] (3) R&S Digital Oscilloscope	CUT: AES-128 Trojan: Small and large Trojans	Euclidean Distance

Another approach of using EM to detect HTs by measuring the backscattered EM radiation from an FPGA was developed by Adibelli et al. [65]. Backscattering is the reflection of EM waves from a surface. In the context of HT detection, the EM waves are generated by an external carrier signal that is modulated by the clock frequency of the IC. The backscattered waves are received by a sensor and analyzed to determine the presence of an HT. The sensor developed in this work consisted of custom E- and H-field probes for inserting the carrier signal and measuring the backscattered emissions respectively. Cyclone V FPGAs, and a Vector Network Analyzer (VNA) were used to detect HTs by measuring the backscattered harmonics of the HT-free and HT-infected circuits with 100% accuracy.

As an improvement to their previous work in [26], He et al. propose an improved golden chip free EM based HT detection approach in [77]. This work addressed the limitations of their earlier approach which only worked when HTs were always active. This extension considered variations in EM emissions caused by different inputs to the CUT. The EM reference model was simulated at the RTL level, considering factors like registers, Look Up Tables (LUTs), fan-out numbers, data

TABLE 2. Summary of EM-based counterfeit detection methods.

Authors	Assurance Method	Experimental Setup	Circuit Under Test (CUT)	Analysis Metrics
Huang *et al.* [82]	Device Identification Using Fingerprinting	(1) Chips: CMOS 0.25 μm (2) Probe: 1-ohm resistor probe (3) MS2667C Spectrum Analyzer	CUT: Digital Circuit Suspect ICs: Modified CUTs for Testing	z-score and R^2 coefficient
Ahmed *et al.* [83]	IC Authentication	(1) Artix-7 and Spartan-3E FPGAs (2) Probe: Langer RF-U 5-2 (3) Digital Oscilloscope	CUT: Ring Oscillators	Cosine Similarity
Stern *et al.* [84]	Remarked & Cloned IC Detection	(1) Function Generator (2) Probe: Langer H-field (3) Mixed Signal Oscilloscope	CUT: 8051 Microcontroller ICs from Atmel, Maxim and NXP	Euclidean, Minkowski & Cityblock Distances
Sayakkara *et al.* [85]	IoT Forensic Investigation	(1) Raspberry Pi and Arduino R3 (2) Probe: H-field probe (3) HackRF SDR (4) Python	CUT: AES-128, AES-256 and 3DES, ROs	Neural Network and SVM
Stern *et al.* [55]	Remarked & Cloned IC Detection	(1) Function Generator (2) Probe: Langer H-field (3) Mixed Signal Oscilloscope (4) 8051 Development Board	CUT: 8051 Microcontroller ICs from Atmel, Maxim, NXP and Gray Market	PCA and LDA
Zhang *et al.* [86]	Device Identification	(1) Test ICs (2) Probe: H-field Probe (3) Digital Oscilloscope (4) IC Evaluation Board	CUT: ICs belonging to various batches	Deep Residual Network
Mariano *et al.* [87]	Device Identification & Software Profiling	(1) Arduino Uno R3 (2) Probe: 6 cm H-field Probe (3) RTL2832U SDR	CUT: Set of Software Programs	Logistic Regression (SBLR)
Kacmarcik *et al.* [88]	Circuit Activity Fingerprinting using Backscattered EM	(1) Cyclone-V FPGA (2) Probe: H-field Probe (3) Keysight N9030B (4) Pasternack PE15A1010 LNA (5) Ansys Electronics Desktop	CUT: Cascaded Inverters, 4-bit Counter, AES-128	Statistical Analysis (mean, variance, skew)

transitions, and drive capabilities of FPGA implementation of the CUT. The study used AES-128 and RSA-128 block ciphers from TrustHub as CUTs on the SAKURA-G platform. Near-field probes and a side-channel analysis setup was used to collect EM traces, and a factor analysis-based feature extraction method followed by k-Means clustering was performed for HT detection.

Zhang et al. [78], [79] also used EM-based side-channel measurements for HT detection. The authors collected EM emissions from FPGAs, comparing changes in emissions with and without HTs. Various circuits, including Trojan-free versions, circuits with small Trojans, and circuits with large Trojans were implemented on an FPGA. The CUT was an AES-128 encryption from the TrustHub repository. EM emissions were gathered from an Altera Cyclone FPGA using a near-field probe [80] and an R&S digital oscilloscope. The authors employed the harmonics of a 100 MHz oscillator on the FPGA to detect HTs, achieving 100% accuracy by analyzing the Euclidean distance between different CUT implementations and assessing differences in oscillator harmonic amplitudes across five FPGAs of the same family.

B. EM-BASED COUNTERFEIT DETECTION

Counterfeit detection generally consists of detection of remarked or cloned ICs which are recycled back into the semiconductor supply chain [8]. Similar to HT detection, EM emissions were used as fingerprints to identify and authenticate circuits and devices for improving the reliability of the system. First, the EM emissions from ICs/FPGAs are measured using a variety of devices, such as an EM probe or an antenna. Once the EM emissions have been measured, they are analyzed to create a unique fingerprint for the device. The fingerprint can then be used to identify the device, even if the device is turned off or has been modified.

In 2014, Huang et al. [82] developed one of the first methods of using unintentional EM emissions for fingerprinting based counterfeit IC detection. The authors demonstrated significant changes in the EM emission profiles of the ICs under test, when they were subjected to accelerated aging

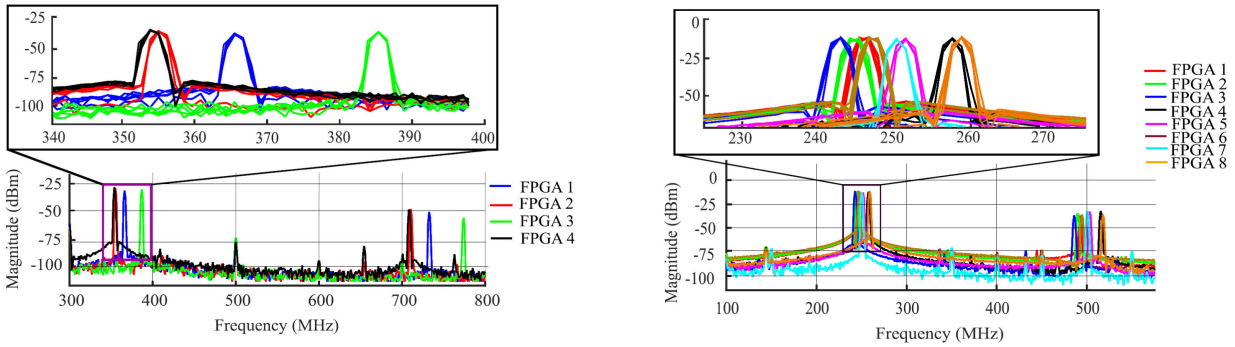

FIGURE 7. EM fingerprints of RO frequencies for 4 Artix-7 and 8 Spartan-3E FPGAs [83] © 2017 IEEE.

tests. EM emission profiles of nine different versions of an authentic digital circuit designed using CMOS 0.25 um process were collected as golden reference fingerprints. EM fingerprints from another set of counterfeit devices were collected for comparison against golden reference. Correlation analysis was performed by comparing z-score or standard score and R^2 coefficient between the reference and suspect devices to observe differences in EM profiles thus detecting counterfeit ICs successfully.

Similar to the above work, Ahmed et al. [83] developed EM fingerprinting based IC authentication method. However, they used a 3-stage ring-oscillator (RO) circuit implemented on two different families of FPGAs at different locations as the CUT. The RO circuit acted as a variability-aware circuit as its oscillation frequency depends on the manufacturing process variations of each FPGA. Unique EM fingerprints could be obtained by analyzing the first harmonics of the oscillation frequencies. Four Artix-7 and eight Spartan-3E FPGAs were used to collect EM fingerprints using a Langer RF-U 5-2 probe and cosine similarity metric was used to analyze uniqueness of the fingerprints across different FPGAs. Auto correlation and cross correlation results showed unique fingerprints for all the CUTs as shown in Fig. 7.

Sayakkara et al. [85] performed EM side-channel analysis on IoT devices for forensic analysis. In this detailed work, the authors performed different experiments and demonstrated that EM radiation can be utilized to understand the internal activities of the devices. The experiments focused on discriminating various cryptographic algorithms running on the device, detection of software behavior and detection of firmware modifications in the device. IoT devices like Raspberry Pi's and Arduino MCUs were programmed with AES-126, AES-256, 3DES, and other algorithms to collect EM data using H-field probe and a HackRF software defined radio (SDR). Huge amounts of labeled EM data was curated and machine learning models including neural networks, and support vector machines (SVM) were utilized to perform the classification. The neural network models classified the cryptographic algorithms with an accuracy of 92% and the SVM model detected the presence of malicious code with 100% accuracy.

Another framework called EMFORCED was proposed by Stern et al. for counterfeit detection in [55] and [84] as shown in Fig. 8. In the first work [84], the authors present EMFORCED framework designed for detecting counterfeit ICs, particularly remarked and cloned ones. This framework is applicable for device authentication without modifying the original IC functionality as it leveraged the unique clock distribution network of each chip to generate design-specific EM fingerprints. The authors used an external pulse (5V peak-to-peak, 50% duty cycle) to stimulate the clock network and collected fingerprints. These fingerprints were compared with golden reference using Principal Component Analysis (PCA) and three distance metrics (Euclidean, Minkowski, City block) to verify authenticity. Experiments using 8051 microcontroller ICs from Atmel, Maxim, and NXP vendors demonstrated over 99% classification accuracy with an unsupervised machine learning model. However, the ICs were only taken from the three vendors with very few test cases. The extension of this work [55] overcame this limitation by including other test chips from gray market and improved analysis methods.

The authors in [55] explored two scenarios for data classification to detect counterfeit ICs: reference-free and reference-inclusive measurements. In reference-free experiments, a custom breadboard setup and a COTS 8051 development board were used, while reference-inclusive measurements exclusively utilized the development board. Both setups maintained the original circuit design, requiring only an external clock pulse for enhanced EM collection. LANGER RF probes were used to collect EM fingerprints. Preprocessing and classification of authentic and suspect chips were achieved through unsupervised (PCA) and supervised (LDA) machine learning models, with high accuracy of 99.46% and 100%, respectively.

With advancements in data analysis methods, researchers utilized novel deep learning architectures to process EM data for counterfeit detection. Zhang et al. [86] developed a method which utilized deep learning for EM data analysis. This work utilized deep residual neural networks to identify and verify ICs. The EM radiation was collected using a near-field probe and a digital oscilloscope. The collected

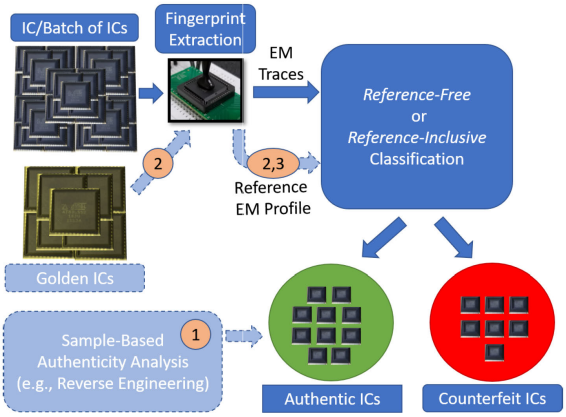

FIGURE 8. EMFORCED framework for counterfeit detection overview [55]

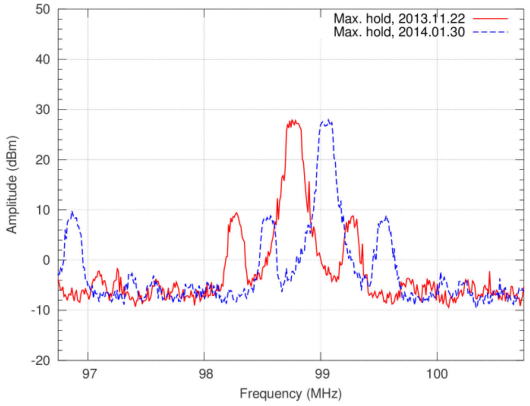

FIGURE 9. EM emission shift from a PIC MCU after aging (blue) [90]

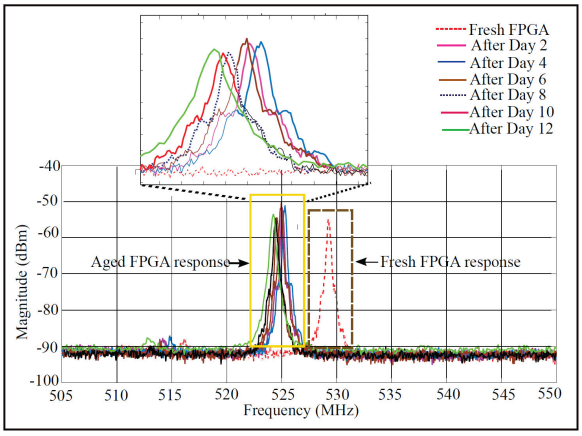

FIGURE 10. Impact of aging on the RO frequencies [91]

data was analyzed and classified by the deep residual neural network without any additional preprocessing or feature extraction steps. The deep learning approach outperformed traditional machine learning algorithms, such as SVM and logistic regression, in terms of classification accuracy.

Unlike previous EM collection methods, a novel multichannel EM data collection was proposed by Mariano et al. [87]. The authors presented a method to uniquely identify Arduino devices and the software running on them using EM fingerprints. This method, inspired by EEG/MEG data collection, used a multichannel data collection setup and a sparse bilinear logistic regression (SBLR) algorithm for device detection and software characterization. It achieved 100% accuracy in device identification and demonstrated promising results in software characterization. The authors discussed possible improvements to enhance the data collection process by increasing the coverage area and collection time.

A golden chip free method of device identification was proposed by Kacmarcik et al. [88] using backscattered EM emissions from an FPGA. Reference fingerprints were generated by simulation using Ansys Electronics Desktop (EDT) that excluded noise and interconnects from its simulation model. Measurements were taken from three circuits (cascaded inverter chain, 4-bit counter, AES) implemented on Cyclone V FPGA using an EM probe connected to a spectrum analyzer. The simulated and measured EM data were compared using various metrics such as mean, variance, maximum match error and skew to determine the circuit identity. Circuit identification was performed with 95% accuracy, demonstrating the effectiveness of this golden chip-free circuit identification method.

A recent survey exclusively on RF-Fingerprinting was given by Miguélez-Gómez and Rojas-Nastrucci [89] which covered the fundamentals of HTs and recent advances in HT detection using fingerprinting with a focus on other RF based fingerprinting methods such as transient, path delay and few EM based methods to improve trustworthiness of hardware.

C. EM-BASED RELIABILITY MONITORING OF ICS

Reliability of an IC, as described earlier, depends on various factors of which circuit aging plays a major role. Researchers have attempted to understand the behavior of EM emissions when the IC or the DUT is subjected to accelerated aging conditions. Studies have shown that EM radiation from circuits and systems change over time due to accelerated aging as the natural degradation phenomenon (BTI, HCI, TDDB) of a device are accelerated under harsh environmental conditions such as high temperature or electrical stress. Understanding the behavior of IC emissions under such conditions can help us estimate the extent of aging of the device and prevent early failures.

To study the impact of thermal stress on the characteristics of of EM emissions, Montanari et al. [92] subjected different power supply units of a personal computer to thermal tests. The study found that aging can modify the electromagnetic signature of electronic devices, but the signature remains identifiable which can be used for device identification, and diagnostics. Observed spectra from the DUTs showed a difference in the switching frequencies of different devices across the groups however, the exact aging could not be assessed based on these changes. Boyer et al. [53] conducted accelerated life time tests to characterize the evolution of IC

emissions after aging. The study found that the four aging tests (high temperature, low temperature, ESD, and load dump) had contrasting EM emission profiles. While HTOL and TC contributed to reducing the emission level, ESD and LD induced an increase of parasitic emissions.

Similar thermal and electrical aging tests were performed on various active and passive devices to study their susceptibility to electromagnetic emissions. Fernandez et al. [93] studied the impact of NBTI on CMOS inverter's EM emissions and found that it can reduce switching noise but does not affect EMI susceptibility. Lafon et al. [94] performed a study to observe the impact of aging on passive components like capacitors and observed that EM emissions increased in contrast to decrease in the IC emission level. Other works by Boyer et al. [95] and Wu et al. [96] show the impact of aging on analog circuit's EM susceptibility. While all the above works show that the EM emissions of active and passive components of ICs do change with accelerated aging, they could not determine the reason for such characteristic behavior. However, another work by Boyer et al. [97] proposed that electrical stress accelerated the mechanisms like NBTI and HCI, leading to a decrease in the transient current amplitude which resulted in the reduction of conducted EM emissions at high frequencies.

Along with active and passive components of ICs, aging tests were performed on other devices like microcontrollers and FPGAs. Dawson et al. [90] studied the impact of thermal aging on the EM emissions of PIC microcontrollers. 8 devices were heated at 140°C for one week in a thermal oven and a measurable shift in emission frequency was observed as seen in Fig. 9. A recent study on EM based FPGA authentication by Ahmed et al. [91] studied the impact of aging on EM fingerprints. For this study, 4 FPGAs from the same family were used to implement ring oscillators (RO) to act as a variation aware CUT to generate fingerprints. The FPGAs were aged on a hot plate by heating them for two weeks at 80°C (equivalent to 4 years aging). The RO frequency decreased (Fig. 10) with aging as the oscillation frequency depends on the process variations and the delay of each inverter in the chain which is impacted by aging.

Recently, Vutukuru and Muha et al. [52] proposed a method to estimate the reliability of an IC using on-chip EM sensors. The method described a way to visualize aging and detecting electromigration of interconnects in an IC using EM emissions. For visualizing aging, a side-channel measurement setup was used to collect EM traces from an FPGA in which an AES-128 encryption, ring-oscillators (RO) and continuously switching HTs were implemented. RO's were used as active aging monitors by measuring the RO frequency in the frequency domain which showed a degradation of the frequency as the CUT aged due to increased HT switching activity. For electromigration detection, the ratio of common mode to differential mode components of the signal was measured as the resistance of the interconnect changed. Simulation results showed that this ratio changed as the resistance of the interconnect increased due to electromigration, providing a way to estimate electromigration in interconnects.

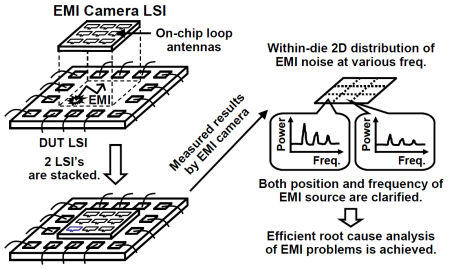

FIGURE 11. On-chip antenna array for EMI measurement [27] © 2010 IEEE.

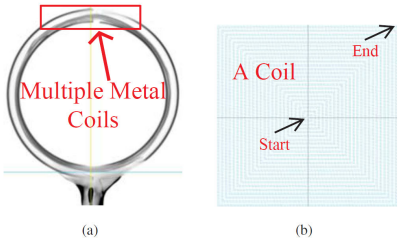

FIGURE 12. Structures of (a) Langer probe; (b) on-chip EM sensor [28] © 2020 IEEE.

Discussion: The summary of all methods for EM-based HT detection, counterfeit detection and reliability monitoring is provided in Tables 1, 2, 3 respectively. The methods cited above focus on off-chip monitoring of EM signals to provide assurance. However, there are several challenges associated with data collection using the side-channel measurement setup. Factors such as the type of probe used, the distance between the probe tip and the chip or DUT, and the probe's orientation play a major role in obtaining high-quality EM data. As the probe measurements are susceptible to environmental noise, few works used anechoic chambers to minimize variations due to external sources [92]. While side-channel measurement setups are useful for non-invasive, off-chip monitoring in laboratory environments, they are not feasible for continuous monitoring of the chip during run-time. Recently, to enable continuous monitoring of ICs, various on-chip antennas or EM-sensors have been proposed for ensuring chip integrity during operation [27], [28], [52], [81].

VI. SUMMARY OF ON-CHIP ANTENNA STRUCTURES FOR EM-BASED HARDWARE ASSURANCE

Masunaga et al. [27] developed EMcam, which consists of a 12 × 4 on-chip antenna array for monitoring EMI noise of ICs as seen in Fig. 11. This sensor worked by first picking up the EMI noise with the on-chip loop antenna array. The EMI noise was down-converted, amplified, and low-pass-filtered. The down-conversion step was important because it reduced the noise and increased the bandwidth of the EMcam. The amplified and filtered noise was then converted to a digital signal by a rectifier and a comparator and the EMI noise was measured. The antenna performance metrics can be seen in Table 4.

TABLE 3. Summary of EM-based reliability monitoring methods.

Authors	Study	Experimental Setup	Device Under Test	Observation
Montanari *et al.* [92]	Impact of thermal stress on conducted emissions	(1) Thermal Aging Setup (2) R&S ESMI Receiver	PC Power Supply Units	Difference in switching frequencies of different devices
Boyer *et al.* [53]	Evolution of IC emissions after aging	(1) Accelerated Aging Setup (2) Climatic Chamber (3) Spectrum Analyzer	eXtreme Switch or E-Switch: Mixed Power Circuit	HOTL and TC tests decreased EM emissions. ESD and LD tests increased EM emissions of DUT
Lafon *et al.* [94]	Influence of aging on EMC of passive components	(1) Simulation Environment (2) Simulation Models	Ceramic Capacitors, Electrolytic Capacitors, Thick film Resistors	EM emissions increased as the passive components were aged in contrast to decrease in emission level observed in ICs
Boyer *et al.* [97]	Effects of electrical stress on EM emissions from ICs	(1) Accelerated Aging Setup (2) Vector Network Analyzer (3) Chip Evaluation Platform	Freescale 90 nm CMOS ICs	Electrical stress accelerated NBTI, HCI => decreased transient current amplitude => reduced conducted emissions at high frequencies
Dawson *et al.* [90]	Effect of high temperature aging on EM from PIC MCU	(1) PIC MCUs (2) Thermal Oven (3) Spectrum Analyzer (4) Battery	PIC Microcontrollers on a test board	Measurable change in EM emission frequency before and after PIC aging
Ahmed *et al.* [91]	Aged Device Identification	(1) Nexys-4: Artix-7 FPGAs (2) Probe: Langer EMV (3) Spectrum Analyzer (4) Hot Plate	CUT: Ring Oscillators (RO)	Reduced RO frequency after aging equivalent to 4 years
Vutukuru & Muha *et al.* [52]	Aging and Electromigration Detection using EM emissions	(1) Artix-7 FPGA (2) Probe: TekBox H-Probe (3) Keysight DSO104A	CUT: AES-128, Ring Oscillators (RO)	Decreased RO frequencies with aging. Detected electromigration using EM emissions

TABLE 4. On-chip antenna performance summary [27].

Antenna Size	250μm x 50μm
Gain	47 dB
Max. Frequency	3.3 GHz
Frequency resolution	3 MHz
Spatial resolution	60μm

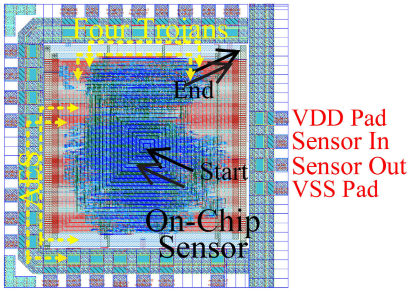

FIGURE 13. On-chip EM sensor layout with AES-128 Fabricated CUT [28] © 2020 IEEE.

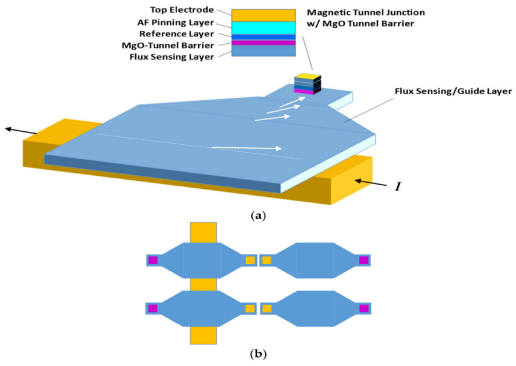

FIGURE 14. (a)The on-chip non-invasive current sensor with magnetic flux guide, concentrator and MTJ (b) bridge sensing structure to eliminate response to field disturbance [81].

To enable HT detection in ICs, He et al. [28] proposed a run-time trust evaluation framework using an on-chip EM sensor. The sensor, inspired by the coil structure of a LANGER RF probe, showed a higher signal-to-noise (SNR) ratio compared to external probes in both simulations and experiments. The fabricated sensor was able to detect the presence of four different types of HTs inserted into an AES-128 encryption circuit with high accuracy. The EM sensor was designed to be placed on the topmost metal layer of the chip. It consists of a coil-like structure similar to that of a LANGER RF probe as depicted in Fig. 12. The sensor was connected to four pads for power, ground, sensor in, and sensor out. The output signal of the sensor was the voltage difference between the start and end points of the coil. The AES-128 chip was fabricated using 180 nm CMOS technology with the proposed EM sensor in the top metal layer as illustrated in Fig. 13. The EM traces were collected

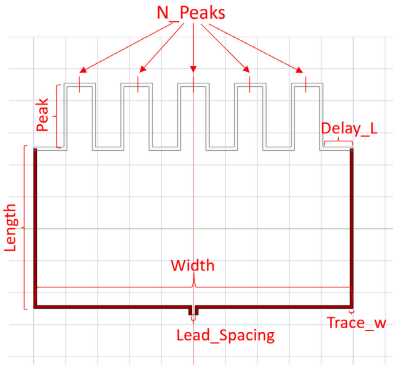

FIGURE 15. On-chip EM sensor array design [52] © 2023 IEEE.

and compared to the simulated reference EM traces to detect the presence of HTs.

Another on-chip sensor design was proposed by Chen et al. (Fig. 14) based on a magnetic tunnel junction (MTJ) [81]. MTJ sensors are a type of non-invasive current sensors that can be used to detect electromagnetic activity on a chip. They are composed of two ferromagnetic layers separated by an insulating layer, and the resistance of the MTJ is dependent on the relative orientation of the magnetization of the two layers. When current flows through the MTJ, it generates a magnetic field that causes the magnetization of the free layer to rotate. The amount of rotation is proportional to the current amplitude, and this rotation can be detected by the MTJ sensor. Using this principle, the authors placed the sensors near critical paths to detect abnormal current patterns. The sensors were characterized and modeled, and the relationship between magnetic field and resistance was determined. Electromagnetic analysis determined the magnetic field each sensor sensed, and Bayesian Neural Network (BNN) classifier was used to detect hardware Trojans accurately.

Vutukuru and Muha et al. [52] proposed a design for an on-chip EM sensor array to measure the EM emissions of ICs for reliability monitoring. They optimized a loop antenna to achieve a lower return loss (|S(1,1)|) and a resonant frequency of 1.5 GHz, to target the typical clock frequency range of ICs or FPGAs. The f_r was reduced by incorporating a meandering structure into the loop antenna, as shown in Fig. 15. Table 5 lists the final optimized values of the loop antenna for the proposed on-chip EM sensor array design. Simulation results suggest that this on-chip EM sensor array could detect electromigration in interconnects by analyzing the ratio of common-mode to differential mode coupling between antenna and the interconnect trace on the IC.

Challenges: Despite the advantages of on-chip antennas for continuous monitoring, various challenges arise during their fabrication, testing and characterization. Common issues observed in on-chip antennas include losses due to the silicon substrate due to its low resistivity and high permittivity, and coupling from neighboring circuits and components. In addition, there is a lack of established design rules for antenna layout. Other challenges also emerge during wafer-level characterization of the antennas due to the testing setup which can introduce reflection, scattering, and coupling effects when using Ground-Signal-Ground (GSG) probes [98], [99], [100], [101]. Additionally, for hardware assurance applications, the antennas must be carefully designed to achieve the required resonant frequency or coupling with interconnects, while also complying with chip size constraints. Techniques like incorporating a meandering structure in the antenna's geometry can help reduce f_r. Moreover, integrating on-chip antenna read-out circuitry introduces additional area and power overhead to the chip. Despite these challenges, when properly optimized, on-chip antennas can significantly improve continuous monitoring and overall reliability of ICs.

TABLE 5. Antenna optimization parameters [52].

Parameter	Optimized value
Length	250 μm
Width	500 μm
Trace_W	5 μm
Lead_Spacing	15 μm
N_Peaks	5
Peak	115 μm
Delay_L	50 μm

VII. FUTURE RESEARCH DIRECTIONS IN EM-BASED HARDWARE ASSURANCE

Future research in EM-based hardware assurance should focus on developing optimized on-chip antenna array designs that offer extensive spatial and temporal coverage. While coupling with interconnects need to be optimized, interference with underlying circuits need to be minimized for extracting meaningful features to provide assurance and aging information during run-time. Additionally, the ability to extract EM fingerprints that reflect foundry-specific manufacturing behaviors across different chip designs could be crucial in determining the foundry of origin for a chip. This approach not only enhances the reliability and security of the ICs but also helps in authenticating IC manufacturing processes.

VIII. CONCLUSION

In this survey, we explored recent advancements in electromagnetic radiation (EM) based hardware assurance methods, including hardware Trojan detection, counterfeit detection, and reliability monitoring. We discussed various assurance methods employing traditional near-field probes and on-chip antenna structures, wherein their advantages and challenges associated with experimental setups are highlighted. The benefits and challenges of on-chip antennas, which is an emerging method for measuring EM emissions to enable continuous monitoring of ICs are explored. The survey finally outlines the future scope of research in developing on-chip antennas to improve feature extraction for foundry of origin detection and aging information during run-time for IC authentication.

ACKNOWLEDGMENT

The authors thank Dr. Marty Emmert, Mr. Luis Concha, and Ms. Donna Longworth for their support.

REFERENCES

[1] B. Daniel. *Counterfeit Electronic Parts: A Multibillion-Dollar Black Market*. Accessed: Apr. 20, 2024. [Online]. Available: https://www.trentonsystems.com/blog/counterfeit-electronic-parts

[2] *Counterfeit Electronic Parts in the Department of Defense Supply Chain*. Accessed: Apr. 20, 2024. [Online]. Available: https://www.govinfo.gov/content/pkg/CHRG-112shrg72702/html/CHRG-112shrg72702.htm

[3] *Elimination of Counterfeiting*. Accessed: Apr. 20, 2024. [Online]. Available: https://agmaglobal.org/About-AGMA/what-we-do/Elimination-Counterfeiting

[4] D. Akhoundov. *2017 Erai Reported Parts Analysis*. Accessed: Apr. 20, 2024. [Online]. Available: https://www.erai.com/erai_blog/3139/_2017_erai_reported_parts_analysis

[5] K. Liakos, G. Georgakilas, and F. Plessas, "Hardware and system security: Attacks and countermeasures against hardware Trojans," in *Frontiers of Quality Electronic Design (QED) AI, IoT and Hardware Security*. Cham, Switzerland: Springer, 2023, pp. 501–549, doi: 10.1007/978-3-031-16344-9_13.

[6] S. Akter, K. Khalil, and M. Bayoumi, "A survey on hardware security: Current trends and challenges," *IEEE Access*, vol. 11, pp. 77543–77565, 2023.

[7] V. Kumar and K. Paul, "Device fingerprinting for cyber-physical systems: A survey," *ACM Comput. Surv.*, vol. 55, no. 14s, pp. 1–41, Jul. 2023, doi: 10.1145/3584944.

[8] E. Oriero and S. R. Hasan, "Survey on recent counterfeit IC detection techniques and future research directions," *Integration*, vol. 66, pp. 135–152, May 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167926018301664

[9] W. Hu, C.-H. Chang, A. Sengupta, S. Bhunia, R. Kastner, and H. Li, "An overview of hardware security and trust: Threats, countermeasures, and design tools," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 40, no. 6, pp. 1010–1038, Jun. 2021.

[10] J. F. Zhang, R. Gao, M. Duan, Z. Ji, W. Zhang, and J. Marsland, "Bias temperature instability of MOSFETs: Physical processes, models, and prediction," *Electronics*, vol. 11, no. 9, p. 1420, Apr. 2022. [Online]. Available: https://www.mdpi.com/2079-9292/11/9/1420

[11] Y. Wang, Y. Li, Y. Yang, and W. Chen, "Hot carrier injection reliability in nanoscale field effect transistors: Modeling and simulation methods," *Electronics*, vol. 11, no. 21, p. 3601, Nov. 2022. [Online]. Available: https://www.mdpi.com/2079-9292/11/21/3601

[12] S.-H. Lee, B.-J. Cho, J.-C. Kim, and S.-H. Choi, "Quasi-breakdown of ultrathin gate oxide under high field stress," in *IEDM Tech. Dig.*, Dec. 1994, pp. 605–608.

[13] T. Gaskin, H. Cook, W. Stirk, R. Lucas, J. Goeders, and B. Hutchings, "Using novel configuration techniques for accelerated FPGA aging," in *Proc. 30th Int. Conf. Field-Program. Log. Appl. (FPL)*, Aug. 2020, pp. 169–175.

[14] S. R. Hasan, S. F. Mossa, O. S. A. Elkeelany, and F. Awwad, "Tenacious hardware trojans due to high temperature in middle tiers of 3-D ICs," in *Proc. IEEE 58th Int. Midwest Symp. Circuits Syst. (MWSCAS)*, Aug. 2015, pp. 1–4.

[15] N. Evmorfopoulos, M. A. A. Shohel, O. Axelou, P. Stoikos, V. A. Chhabria, and S. S. Sapatnekar, "Recent progress in the analysis of electromigration and stress migration in large multisegment interconnects," in *Proc. Int. Symp. Phys. Design*, New York, NY, USA, 2023, pp. 115–123, doi: 10.1145/3569052.3578919.

[16] A. Amouri, F. Bruguier, S. Kiamehr, P. Benoit, L. Torres, and M. Tahoori, "Aging effects in FPGAs: An experimental analysis," in *Proc. 24th Int. Conf. Field Program. Log. Appl. (FPL)*, Sep. 2014, pp. 1–4.

[17] Z. Ghaderi, M. Ebrahimi, Z. Navabi, E. Bozorgzadeh, and N. Bagherzadeh, "SENSIBle: A highly scalable SENsor DeSIgn for path-based age monitoring in FPGAs," *IEEE Trans. Comput.*, vol. 66, no. 5, pp. 919–926, May 2017.

[18] M. D. Valdes-Peña, J. Fernández Freijedo, M. J. Moure Rodríguez, J. J. Rodríguez-Andina, J. Semião, I. M. C. Teixeira, J. P. C. Teixeira, and F. Vargas, "Design and validation of configurable online aging sensors in nanometer-scale FPGAs," *IEEE Trans. Nanotechnol.*, vol. 12, no. 4, pp. 508–517, Jul. 2013.

[19] D. Sengupta and S. S. Sapatnekar, "Predicting circuit aging using ring oscillators," in *Proc. 19th Asia South Pacific Design Autom. Conf. (ASP-DAC)*, Jan. 2014, pp. 430–435.

[20] L. Lanzieri, G. Martino, G. Fey, H. Schlarb, T. C. Schmidt, and M. Wählisch, "A review of techniques for ageing detection and monitoring on embedded systems," 2023, *arXiv:2301.06804*.

[21] K. Arvin and R. Jha, "Aging prediction of integrated circuits using ring oscillators and machine learning," in *Proc. IEEE Phys. Assurance Inspection Electron. (PAINE)*, Nov. 2021, pp. 1–8.

[22] G. Muha, J. Mayersky, and R. Jha, "Low-overhead in-situ aging monitors using a reconfigurable FeFET for trusted hardware," in *Proc. IEEE Nat. Aerosp. Electron. Conf. (NAECON)*, Aug. 2021, pp. 239–242.

[23] J.-J. Quisquater and D. Samyde, "Electromagnetic analysis (EMA): Measures and counter-measures for smart cards," in *Smart Card Programming and Security*, I. Attali and T. Jensen, Eds. Berlin, Germany: Springer, 2001, pp. 200–210.

[24] A. Sayakkara, N.-A. Le-Khac, and M. Scanlon, "A survey of electromagnetic side-channel attacks and discussion on their case-progressing potential for digital forensics," *Digit. Invest.*, vol. 29, pp. 43–54, Jun. 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1742287618303840

[25] J. He, X. Guo, M. Tehranipoor, A. Vassilev, and Y. Jin, "EM side channels in hardware security: Attacks and defenses," *IEEE Des. Test*, vol. 39, no. 2, pp. 100–111, Apr. 2022.

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

[27] N. Masunaga, K. Ishida, M. Takamiya, and T. Sakurai, "EMI camera LSI (EMcam) with 12×4 on-chip loop antenna matrix in 65-nm CMOS to measure EMI noise distribution with 60-μm spatial precision," in *Proc. IEEE Custom Integr. Circuits Conf.*, Sep. 2010, pp. 1–4.

[28] 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 *Proc. 57th ACM/IEEE Design Autom. Conf. (DAC)*, Jul. 2020, pp. 1–6.

[29] A. Ghosh, M. Nath, D. Das, S. Ghosh, and S. Sen, "Electromagnetic analysis of integrated on-chip sensing loop for side-channel and fault-injection attack detection," *IEEE Microw. Wireless Compon. Lett.*, vol. 32, no. 6, pp. 784–787, Jun. 2022.

[30] Y. Miura and Y. Matukura, "Investigation of silicon-silicon dioxide interface using MOS structure," *Jpn. J. Appl. Phys.*, vol. 5, no. 2, p. 180, Feb. 1966, doi: 10.1143/jjap.5.180.

[31] T. H. Ning, P. W. Cook, R. H. Dennard, C. M. Osburn, and S. Schuster, "1 μm MOSFET VLSI technology. IV. Hot-electron design constraints," *IEEE J. Solid-State Circuits*, vol. SSC-14, no. 2, pp. 268–275, Apr. 1979. [Online]. Available: https://api.semanticscholar.org/CorpusID:20179400

[32] C. Hu, S. C. Tam, F.-C. Hsu, P.-K. Ko, T.-Y. Chan, and K. W. Terrill, "Hot-electron-induced MOSFET degradation–model, monitor, and improvement," *IEEE J. Solid-State Circuits*, vol. SSC-20, no. 1, pp. 295–305, Feb. 1985.

[33] J. S. Suehle, "Ultrathin gate oxide reliability: Physical models, statistics, and characterization," *IEEE Trans. Electron Devices*, vol. 49, no. 6, pp. 958–971, Jun. 2002.

[34] J. H. Stathis, M. Wang, and K. Zhao, "Reliability of advanced high-k/metal-gate n-FET devices," *Microelectron. Rel.*, vol. 50, nos. 9–11, pp. 1199–1202, Sep. 2010. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0026271410002908

[35] D. K. Schroder and J. A. Babcock, "Negative bias temperature instability: Road to cross in deep submicron silicon semiconductor manufacturing," *J. Appl. Phys.*, vol. 94, no. 1, pp. 1–18, Jun. 2003, doi: 10.1063/1.1567461.

[36] M. A. Alam and S. Mahapatra, "A comprehensive model of PMOS NBTI degradation," *Microelectron. Rel.*, vol. 45, no. 1, pp. 71–81, Jan. 2005. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0026271404001751

[37] V. Huard, M. Denais, and C. Parthasarathy, "NBTI degradation: From physical mechanisms to modelling," *Microelectron. Rel.*, vol. 46, no. 1, pp. 1–23, Jan. 2006. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0026271405000351

[38] J. H. Stathis and S. Zafar, "The negative bias temperature instability in MOS devices: A review," *Microelectron. Rel.*, vol. 46, nos. 2–4, pp. 270–286, Feb. 2006. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0026271405003008

[39] X. Yang, Q. Sang, C. Wang, M. Yu, and Y. Zhao, "Development and challenges of reliability modeling from transistors to circuits," *IEEE J. Electron Devices Soc.*, vol. 11, pp. 179–189, 2023.

[40] E. Takeda, N. Suzuki, and T. Hagiwara, "Device performance degradation to hot-carrier injection at energies below the Si-SiO_2energy barrier," in *IEDM Tech. Dig.*, Dec. 1983, pp. 396–399.

[41] S. Rangan, N. Mielke, and E. Yeh, "Universal recovery behavior of negative bias temperature instability [PMOSFETs]," in *IEDM Tech. Dig.*, Dec. 2003, p. 14.3.1.

[42] M. Ershov, S. Saxena, H. Karbasi, S. Winters, S. Minehane, J. Babcock, R. Lindley, P. Clifton, M. Redford, and A. Shibkov, "Dynamic recovery of negative bias temperature instability in p-type metal–oxide–semiconductor field-effect transistors," *Appl. Phys. Lett.*, vol. 83, no. 8, pp. 1647–1649, Aug. 2003, doi: 10.1063/1.1604480.

[43] B. Weir, P. Silverman, D. Monroe, K. Krisch, M. Alam, G. Alers, T. Sorsch, G. Timp, F. Baumann, C. Liu, Y. Ma, and D. Hwang, "Ultra-thin gate dielectrics: They break down, but do they fail?" in *IEDM Tech. Dig.*, Dec. 1997, pp. 73–76.

[44] T. Nigam, K.-Y. Yiang, and A. Marathe, "Moore's law: Technology scaling and reliability challenges," in *Microelectronics to Nanoelectronics: Materials, Devices & Manufacturability*, 2012, p. 1.

[45] K. N. Tu and A. N. Gusak, "Mean-time-to-failure equations for electromigration, thermomigration, and stress migration," *IEEE Trans. Compon., Packag., Manuf. Technol.*, vol. 10, no. 9, pp. 1427–1431, Sep. 2020.

[46] K. K. Kim, "Analysis of electromigration in nanoscale CMOS circuits," *J. Korea Ind. Inf. Syst. Res.*, vol. 18, no. 1, pp. 19–24, 2013.

[47] J. Lienig, "Introduction to electromigration-aware physical design," in *Proc. Int. Symp. Phys. Design*, New York, NY, USA, 2006, pp. 39–46, doi: 10.1145/1123008.1123017.

[48] B. Geden, "Understand and avoid electromigration (EM) & IR-drop in custom IP blocks," Synop., White Paper, 2011, pp. 1–6.

[49] J. Black, "Electromigration—A brief survey and some recent results," *IEEE Trans. Electron Devices*, vol. ED-16, no. 4, pp. 338–347, Apr. 1969.

[50] J. Lienig and M. Thiele, *Fundamentals of Electromigration*. Cham, Switzerland: Springer, 2018, pp. 13–60, doi: 10.1007/978-3-319-73558-0_2.

[51] K.-D. Lee, J. Kim, T.-Y. Jeong, Y. Zhao, Q. Yuan, A. Patel, Z. T. Mai, L. H. Brown, S. English, and D. Sawyer, "Effect of Joule heating on electromigration in dual-damascene copper low-k interconnects," in *Proc. IEEE Int. Rel. Phys. Symp. (IRPS)*, Apr. 2017, pp. 6B-6.1–6B-6.5.

[52] M. Y. Vutukuru, A. Muha, and R. Jha, "On-chip EM sensor arrays for reliability monitoring of integrated circuits," in *Proc. IEEE Nat. Aerosp. Electron. Conf. (NAECON)*, Aug. 2023, pp. 157–162.

[53] A. Boyer, A. C. Ndoye, S. Ben Dhia, L. Guillot, and B. Vrignon, "Characterization of the evolution of IC emissions after accelerated aging," *IEEE Trans. Electromagn. Compat.*, vol. 51, no. 4, pp. 892–900, Nov. 2009.

[54] M. Ramdani, E. Sicard, A. Boyer, S. B. Dhia, J. J. Whalen, T. H. Hubing, M. Coenen, and O. Wada, "The electromagnetic compatibility of integrated circuits—Past, present, and future," *IEEE Trans. Electromagn. Compat.*, vol. 51, no. 1, pp. 78–100, Feb. 2009.

[55] A. Stern, U. Botero, F. Rahman, D. Forte, and M. Tehranipoor, "EMFORCED: EM-based fingerprinting framework for remarked and cloned counterfeit IC detection using machine learning classification," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 28, no. 2, pp. 363–375, Feb. 2020.

[56] M. Lacruche and P. Maurine, "Electromagnetic activity vs. Logical activity: Near field scans for reverse engineering," in *Smart Card Research and Advanced Applications*, B. Bilgin and J.-B. Fischer, Eds. Cham, Switzerland: Springer, 2019, pp. 140–155.

[57] J. Huan, P. Dehghanzadeh, S. Mandal, and S. Bhunia, "Contact-less integrity verification of microelectronics using near-field EM analysis," *IEEE Access*, vol. 11, pp. 80588–80599, 2023.

[58] B. Deutschmann, H. Pitsch, and G. Langer, "Near field measurements to predict the electromagnetic emission of integrated circuits," in *Proc. 5th Int. Workshop Electromagn. Compat. Integr. Circuits*, 2005, pp. 27–32.

[59] D. Wang, X.-C. Wei, E.-X. Liu, and R. X.-K. Gao, "Probe design and source reconstruction for near-field scanning and modeling," *IEEE Electromagn. Compat. Mag.*, vol. 12, no. 1, pp. 75–86, 1st Quart., 2023.

[60] J. Daemen and V. Rijmen, *AES Proposal: Rijndael*, document, National Institute of Standards and Technology (NIST), Sep. 1999. [Online]. Available: https://csrc.nist.gov/csrc/media/projects/cryptographic-standards-and-guidelines/documents/aes-development/rijndael-ammended.pdf

[61] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 26, no. 1, pp. 96–99, Jan. 1983, doi: 10.1145/357980.358017.

[62] G. Li, K. Itou, Y. Katou, N. Mukai, D. Pommerenke, and J. Fan, "A resonant E-field probe for RFI measurements," *IEEE Trans. Electromagn. Compat.*, vol. 56, no. 6, pp. 1719–1722, Dec. 2014.

[63] E. Song and H. H. Park, "A high-sensitivity electric probe based on board-level edge plating and LC resonance," *IEEE Microw. Wireless Compon. Lett.*, vol. 24, no. 12, pp. 908–910, Dec. 2014.

[64] F. Fiori and F. Musolino, "Comparison of IC conducted emission measurement methods," *IEEE Trans. Instrum. Meas.*, vol. 52, no. 3, pp. 839–845, Jun. 2003.

[65] S. Adibelli, P. Juyal, L. N. Nguyen, M. Prvulovic, and A. Zajic, "Near-field backscattering-based sensing for hardware trojan detection," *IEEE Trans. Antennas Propag.*, vol. 68, no. 12, pp. 8082–8090, Dec. 2020.

[66] J. Danial, D. Das, S. Ghosh, A. Raychowdhury, and S. Sen, "SCNIFFER: Low-cost, automated, efficient electromagnetic side-channel sniffing," *IEEE Access*, vol. 8, pp. 173414–173427, 2020.

[67] D. Das and S. Sen, "Electromagnetic and power side-channel analysis: Advanced attacks and low-overhead generic countermeasures through white-box approach," *Cryptography*, vol. 4, no. 4, p. 30, Oct. 2020. [Online]. Available: https://www.mdpi.com/2410-387X/4/4/30

[68] M. Y. Vutukuru, A. Muha, R. Srinivasan, and R. Jha, "Impact of CMOS BEOL and heterogenous packaging process conditions on the performance of on-chip antenna arrays for EM radiation monitoring," in *Proc. IEEE Nat. Aerosp. Electron. Conf. (NAECON)*, Jul. 2024, pp. 297–300.

[69] M. Tehranipoor and F. Koushanfar, "A survey of hardware trojan taxonomy and detection," *IEEE Design Test Comput.*, vol. 27, no. 1, pp. 10–25, Jan./Feb. 2010.

[70] Y. Hayashi and S. Kawamura, "Survey of hardware trojan threats and detection," in *Proc. Int. Symp. Electromagn. Compat. (EMC Eur.)*, Sep. 2020, pp. 1–5.

[71] O. Söll, T. Korak, M. Muehlberghuber, and M. Hutter, "EM-based detection of hardware trojans on FPGAs," in *Proc. IEEE Int. Symp. Hardw.-Oriented Secur. Trust (HOST)*, May 2014, pp. 84–87.

[72] J. Balasch, B. Gierlichs, and I. Verbauwhede, "Electromagnetic circuit fingerprints for hardware trojan detection," in *Proc. IEEE Int. Symp. Electromagn. Compat. (EMC)*, Aug. 2015, pp. 246–251.

[73] *Trusthub*. Accessed: Apr. 25, 2024. [Online]. Available: https://trust-hub.org/#/benchmarks/chip-level-trojan

[74] Y. Liu, Y. Zhao, J. He, A. Liu, and R. Xin, "SCCA: Side-channel correlation analysis for detecting hardware trojan," in *Proc. 11th IEEE Int. Conf. Anti-Counterfeiting, Secur., Identificat. (ASID)*, Oct. 2017, pp. 196–200.

[75] R. M. Fuller, R. A. Riley, and J. T. Graham, "Exploiting side-channel emissions to detect changes in FPGA firmware," in *Cyber Sensing*, vol. 10630, I. V. Ternovskiy and P. Chin, Eds. Bellingham, WA, USA: SPIE, 2018, Art. no. 106300A, doi: 10.1117/12.2304450.

[76] Z. Chen, S. Guo, J. Wang, Y. Li, and Z. Lu, "Toward FPGA security in IoT: A new detection technique for hardware trojans," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 7061–7068, Aug. 2019.

[77] J. He, H. Ma, Y. Liu, and Y. Zhao, "Golden chip-free trojan detection leveraging trojan trigger's side-channel fingerprinting," *ACM Trans. Embedded Comput. Syst.*, vol. 20, no. 1, pp. 1–18, Dec. 2020, doi: 10.1145/3419105.

[78] F. Zhang, D. Zhang, Z. Peng, Q. Ren, A. Chen, and D. Su, "Hardware trojan recognition based on radiated emission characteristics," in *Proc. Asia–Pacific Int. Symp. Electromagn. Compat. (APEMC)*, Sep. 2022, pp. 82–84.

[79] F. Zhang, D. Zhang, Q. Ren, A. Chen, and D. Su, "Analytical models of on-chip hardware trojan detection based on radiated emission characteristics," *Chin. J. Electron.*, vol. 33, no. 2, pp. 385–392, Mar. 2024.

[80] J. Wang, Z. Yan, C. Fu, Z. Ma, and J. Liu, "Near-field precision measurement system of high-density integrated module," *IEEE Trans. Instrum. Meas.*, vol. 70, pp. 1–9, 2021.

[81] E. Chen, J. Kan, B.-Y. Yang, J. Zhu, and V. Chen, "Intelligent electromagnetic sensors for non-invasive trojan detection," *Sensors*, vol. 21, no. 24, p. 8288, Dec. 2021. [Online]. Available: https://www.mdpi.com/1424-8220/21/24/8288

[82] H. Huang, A. Boyer, and S. B. Dhia, "The detection of counterfeit integrated circuit by the use of electromagnetic fingerprint," in *Proc. Int. Symp. Electromagn. Compat.*, Sep. 2014, pp. 1118–1122.

[83] M. M. Ahmed, D. Hely, N. Barbot, R. Siragusa, E. Perret, M. Bernier, and F. Garet, "Radiated electromagnetic emission for integrated circuit authentication," *IEEE Microw. Wireless Compon. Lett.*, vol. 27, no. 11, pp. 1028–1030, Nov. 2017.
[84] A. Stern, U. Botero, B. Shakya, H. Shen, D. Forte, and M. Tehranipoor, "EMFORCED: EM-based fingerprinting framework for counterfeit detection with demonstration on remarked and cloned ICs," in *Proc. IEEE Int. Test Conf. (ITC)*, Oct. 2018, pp. 1–9.
[85] A. Sayakkara, N.-A. Le-Khac, and M. Scanlon, "Leveraging electromagnetic side-channel analysis for the investigation of IoT devices," *Digit. Invest.*, vol. 29, pp. S94–S103, Jul. 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1742287619301616
[86] H. Zhang, J. Liu, J. Xu, F. Zhang, X. Cui, and S. Sun, "Electromagnetic radiation-based IC device identification and verification using deep learning," *EURASIP J. Wireless Commun. Netw.*, vol. 2020, no. 1, p. 206, 2020.
[87] L. J. Mariano, A. Aubuchon, T. Lau, O. Ozdemir, T. Lazovich, and J. Coakley, "Classification of electronic devices and software processes via unintentional electronic emissions with neural decoding algorithms," *IEEE Trans. Electromagn. Compat.*, vol. 62, no. 2, pp. 470–477, Apr. 2020.
[88] A. S. Kacmarcik, P. Juyal, M. Prvulovic, and A. Zajic, "Circuit activity fingerprinting using electromagnetic side-channel sensing and digital circuit simulations," *IEEE Access*, vol. 10, pp. 123316–123327, 2022.
[89] N. Miguélez-Gómez and E. A. Rojas-Nastrucci, "RF fingerprinting: hardware-trustworthiness enhancement in the hardware trojan era: RF fingerprinting-based countermeasures," *IEEE Microw. Mag.*, vol. 24, no. 11, pp. 35–52, Nov. 2023.
[90] J. F. Dawson, I. D. Flintoft, A. P. Duffy, A. C. Marvin, and M. P. Robinson, "Effect of high temperature ageing on electromagnetic emissions from a PIC microcontroller," in *Proc. Int. Symp. Electromagn. Compat.*, Sep. 2014, pp. 1139–1143.
[91] M. M. Ahmed, D. Hely, N. Barbot, R. Siragusa, E. Perret, M. Bernier, and F. Garet, "Towards a robust and efficient EM based authentication of FPGA against counterfeiting and recycling," in *Proc. 19th Int. Symp. Comput. Archit. Digit. Syst. (CADS)*, Dec. 2017, pp. 1–6.
[92] I. Montanari, A. Tacchini, and M. Maini, "Impact of thermal stress on the characteristics of conducted emissions," in *Proc. IEEE Int. Symp. Electromagn. Compat.*, Aug. 2008, pp. 1–4.
[93] R. Fernandez, N. Berbel, I. Gil, and M. Morata, "Impact of NBTI on EMC behaviours of CMOS inverter," in *Proc. Asia–Pacific Int. Symp. Electromagn. Compat.*, Apr. 2010, pp. 1020–1023.
[94] F. Lafon, F. De Daran, L. Caves, M. Ramdani, and M. Drissi, "Influence of aging and environnement conditions on emc performances of electronic equipment-influence of passive vs active components," in *Proc. EMC Eur.*, 2010.
[95] A. Boyer, S. Ben Dhia, B. Li, C. Lemoine, and B. Vrignon, "Prediction of long-term immunity of a phase-locked loop," *J. Electron. Test.*, vol. 28, no. 6, pp. 791–802, Dec. 2012.
[96] J. Wu, J. Li, R. Shen, A. Boyer, and S. Ben Dhia, "Effect of electrical stresses on the susceptibility of a voltage regulator," in *Proc. Int. Symp. Electromagn. Compat.*, Sep. 2013, pp. 759–764.
[97] A. Boyer, S. B. Dhia, B. Li, N. Berbel, and R. Fernandez-Garcia, "Experimental investigations into the effects of electrical stress on electromagnetic emission from integrated circuits," *IEEE Trans. Electromagn. Compat.*, vol. 56, no. 1, pp. 44–50, Feb. 2014.
[98] H. M. Cheema and A. Shamim, "The last barrier: On-chip antennas," *IEEE Microw. Mag.*, vol. 14, no. 1, pp. 79–91, Jan. 2013.
[99] S. Mandal, S. K. Mandal, and A. K. Mal, "On-chip antennas using standard CMOS technology: A brief overview," in *Proc. Int. Conf. Innov. Electron., Signal Process. Commun. (IESC)*, Apr. 2017, pp. 74–78.
[100] M. R. Karim, X. Yang, and M. F. Shafique, "On chip antenna measurement: A survey of challenges and recent trends," *IEEE Access*, vol. 6, pp. 20320–20333, 2018.
[101] H. Singh and S. K. Mandal, "Current trends and future perspective of designing on-chip antennas," *Int. J. Microw. Wireless Technol.*, vol. 15, no. 3, pp. 535–545, Apr. 2023.

MANOJ YASASWI VUTUKURU (Graduate Student Member, IEEE) received the bachelor's degree in ECE from the Sreenidhi Institute of Science and Technology (SNIST), Hyderabad, India, in 2018, and the master's degree in electrical and computer engineering from the University of Florida, Gainesville, USA, in 2021. He is currently pursuing the Ph.D. degree with the Department of Electrical and Computer Engineering, University of Cincinnati, Cincinnati, OH, USA. His research interests include hardware security, trust, and reliability, VLSI design, and machine learning for hardware assurance.

JOHN M. (MARTY) EMMERT (Senior Member, IEEE) was born in Lexington, KY, USA. He received the B.Sc. degree in electrical engineering from the University of Kentucky, the M.Sc. degree in electrical engineering from the Air Force Institute of Technology, the Ph.D. degree in computer science and engineering from the University of Cincinnati, and the degree from the Air War College. He is currently a Professor with the Department of Electrical Engineering and Computer Science, University of Cincinnati, and the Director of the NSF Center for Hardware and Embedded Systems Security and Trust (CHEST), I/UCRC. He is a retired Colonel at U.S. Air Force Reserves. He has seven U.S. patents and has directed more than 32M$ in research funding. He and his colleagues were a recipient of the five phase II Small Business Innovative Research contracts from the Department of Defense, the IEEE Harold Nobel Award, and the AFRL Sensors Directorate James B. Tsui Award for Best Patent.

RASHMI JHA (Member, IEEE) received the B.Tech. degree in electrical engineering from IIT Kharagpur, India, in 2000, and the M.S. and Ph.D. degrees in electrical engineering from North Carolina State University, in 2003 and 2006, respectively. She was a Process Integration Engineer of advanced CMOS technologies with IBM Microelectronics, from 2006 to 2008. She is currently an Associate Professor with the Department of Electrical Engineering and Computing Systems, University of Cincinnati. She is also the Director of the Microelectronics and Integrated Systems, Neuro-Centric Devices (MIND) Laboratory, University of Cincinnati. She has been granted 12 U.S. patents and has authored/co-authored several publications. Her current research interests include artificial intelligence, cybersecurity, neuromorphic SoC, emerging logic and memory devices, hardware security, and neuroelectronics. She was a recipient of the Summer Faculty Fellowship Award from AFOSR, in 2017, the CAREER Award from the National Science Foundation (NSF), in 2013, the IBM Faculty Award, in 2012, and the IBM Invention Achievement Award, in 2007.