EMFORCED: EM-based Fingerprinting Framework for Counterfeit Detection with Demonstration on Remarked and Cloned ICs

Andrew Stern, Ulbert Botero, Bicky Shakya, Haoting Shen, Domenic Forte, and Mark Tehranipoor
Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL 32611 USA
{andrew.stern,jbot2016,bshakya}@ufl.edu, {htshen,dforte,tehranipoor}@ece.ufl.edu

***Abstract*—Today's globalized electronics supply chain is prone to counterfeit chip proliferation. Existing techniques to detect counterfeit integrated circuits (ICs) are limited by relatively high cost, lengthy inspection time, destructive nature, and restriction to a pre-packaging environment. We propose a novel method of counterfeit IC detection which takes advantage of design-specific electromagnetic (EM) fingerprints generated by simulating on-chip clock distribution networks. Through exploitation of the chip's physical characteristics, our technique can help detect foundry of origin. We validate our approach on 8051 microcontrollers from three different vendors and utilize principal component analysis to distinguish the acquisitions by vendor. Our results show that near-field EM measurements combined with unsupervised machine learning provide $\approx 99\%$ accuracy in counterfeit detection through design-specific fingerprint classification.**

I. Introduction

The globalized nature of the semiconductor supply chain has made counterfeit integrated circuits (ICs) a pervasive problem. Such ICs undermine the safety, reliability, and security of electronic systems. Counterfeits can be broadly classified into the following categories: recycled, remarked, overproduced, cloned, out-of-spec and defective [1]. Among them, remarked ICs have become particularly concerning and, at the same time, highly lucrative for counterfeiters. Remarked ICs are defined as those whose packaging labels and/or die markings have been modified to misidentify their grade (e.g., commercial, industrial, military, and space grade) or design (e.g., an older processor chip design being remarked as newer version). Together with recycled ICs, they contribute to as much as 80% of all counterfeit ICs discovered in the global semiconductor supply chain thus far [1]. Cloned chips are also slowly becoming a pervasive issue. In chip-level cloning, a reverse engineering team, an untrusted foundry, or a semiconductor design house pirates semiconductor intellectual property (IP) in order to design/produce chips that violate the legitimate owner's rights. This leads to revenue loss and even inclusion of potential backdoors or hardware Trojans in the cloned chips.

The most prevalent methods of detecting counterfeit ICs are physical and electrical inspections [2], [3]. Physical inspection includes destructive and non-destructive methods such as optical/SEM/TEM imaging, chemical composition analysis and X-ray tomography, which try to uncover counterfeit defects and anomalies of remarking (e.g., blacktop coating, corroded pins, etc.)[3]. Unfortunately, such techniques are costly, labor intensive, and can only be applied on a sampling basis. Electrical tests measure the parametric and/or functional characteristics of the ICs under test, usually compared against a known-authentic or 'golden' sample. Unlike physical inspection, electrical tests can be performed quickly on a large batch of ICs from a given lot. Unfortunately, they usually require expensive automatic test equipment (ATE), probe stations, and extensive measurement testbenches. Electronic chip ID (ECID) [4], DNA markings [1], [5], and physical unclonable functions (PUFs) [6], [7] have also been proposed for cloned and remarked chip detection. However, PUFs incur additional overhead, are susceptible to reliability issues, and are not applicable to legacy parts. On the other hand, DNA markings printed on chip packaging are not inherently tied to the underlying die/design within and also require lab characterization for high-confidence verification. Further, ECID does not exist on many legacy parts.

In this paper, we propose a low-cost and easy-to-implement alternative to traditional electrical tests for the detection of counterfeit ICs called EMFORCED. It leverages near-field electromagnetic (EM) probes to generate design-specific fingerprints. These fingerprints enable customers of commercial-off-the-shelf (COTS) chips to verify the origin and therefore, authenticity of the underlying design[1].

EMFORCED includes stimulation of reference chips with an external clock signal, recording of the resulting EM emanation from the clock distribution network and principal component analysis (PCA) based classification to match a chip under test (CUT) with the EM profiles of the reference chips. We demonstrate that such a technique allows customers (original equipment manufacturers (OEMs) or test labs) to build a vendor and design-specific EM profile which allows remarked and cloned ICs to be detected on-the-fly. In contrast to traditional electrical tests, EMFORCED only requires a low-cost EM probe and leverages design-intrinsic features (i.e., the clock tree) for rapid counterfeit IC detection. Additionally, it does not require any test vectors, programs or additional circuitry to be loaded onto the CUT, and can be widely applied to all synchronous digital designs. Further, unlike most prevalent physical inspection techniques, EMFORCED does not require decapping or sample preparation, and can be readily applied to packaged ICs. Our main contributions can be summarized as follows.

- We propose a novel EM based framework for counterfeit IC detection without the need to fully activate the chip functionality, making it applicable to all types of synchronous integrated circuits. To achieve this objective, we stimulate the CUT's clock distribution network to produce EM emissions created by internal transitions for chip design fingerprinting.
- EMFORCED, an EM fingerprinting framework, is detailed along with its potential use for detecting different counterfeit types, with a demonstration on remarked and cloned ICs. Rationale for using EM emission from clock trees is also provided.
- We present PCA-based unsupervised machine learning results on time-series EM measurements collected from 30 8051 microcontrollers (spanning 3 different vendors). The results demonstrate the possibility of forming clearly separable clusters for manufacturer/design specific fingerprints.

The remainder of the paper is organized as follows. Section II discusses related techniques for counterfeit IC detection and their limitations. Section III introduces EMFORCED, our general EM-based framework for combating various types of counterfeit ICs, along with discussion of applicable threat models for each counterfeit type. Section IV provides an overview of EM emissions in ICs, particularly through switching activity via the clock tree. Section V describes our experimental test-bed for EM fingerprint extraction. Section VI presents the classification results along with analysis related to the variation of experimental parameters. Section VII explores the benefits of expanding this methodology to multi-parameter classification. Section VIII discusses developments which could occur in the future to advance the work presented here. Finally, Section IX concludes the paper.

II. Related Work

Modern solutions for detecting counterfeit ICs fall into the following categories: (1) use of design-for-anti-counterfeit (DfAC) technologies, (2) physical inspection and (3) electrical testing using functional test, structural test, and side channel measurement. Among them, DfAC technologies can be used exclusively on new chips while physical inspection can be done on all chips (new and legacy), but can be quite expensive and time consuming. Functional tests and structural tests using scan are expensive as they require a costly tester and knowledge of test patterns. Solutions utilizing side-channel measurements are the most viable low-cost methods. Among the various side-channels that exist in an IC, EM is the most attractive due to its low cost, speed, and ability to resolve spatial emissions data across various regions of the die/chip, with or without test vectors.

Various techniques have also been proposed for the detection of counterfeit ICs and for attesting their origin (e.g., fab, design house). In [8], wafer-level parametric measurements were leveraged in order to assess the foundry of origin of a given die. The authors presented various scenarios where a customer wants to verify in which of the N foundries the die (or batch of dies) were fabricated. While their technique allows foundry characterization and identification without relying on the design underneath the die, their experiments were based on large datasets from pre-packaging die level measurements, and it is unknown whether the collected profiles would retain their accuracy post-packaging. Combating Die and IC Recycling (CDIR) sensors, based on aging-sensitive ring oscillators, have been proposed in [9] for recycled IC detection. However they require integration into the chip at the design stage and are not applicable to legacy parts. Measurement-based approaches relying on aging of SRAM cells [10], lookup table (LUT) path delay characterization [11] and partial programming of flash memory cells [12] have also been proposed to detect recycled ICs. However, these approaches require

[1] We assume that the chip under investigation does not contain ECID or PUF.

enrollment and/or device-specific measurement setups, thus limiting their applicability (e.g., to SoCs with embedded SRAM or exclusively FPGAs). The authors in [13] proposed an EM-based fingerprinting approach for detection of counterfeit ICs (recycled, remarked and cloned). However, their analysis relied on measurements of a mixed signal chip, and used statistical similarity measures to compare the frequency-domain EM profiles of suspect and known-authentic ICs. They also used device-specific on-board configurations to generate underlying transient effects. In contrast, we utilize the easily accessed clock distribution network for fingerprint generation, and analyze both frequency and time-domain signals. Additionally, we perform our measurements on common, COTS digital ICs (i.e., 8051 microcontrollers) and use unsupervised machine learning for fingerprinting and classification. It should be noted that there is also a body of work which leverages EM emissions for the detection of hardware Trojans [14] and malwares [15], generating watermarks [16] and performing side-channel analysis on cryptocores [17]. Given the widespread utility of EM emission analysis, we consider our work to be complementary to these approaches for countering various semiconductor supply chain threats.

III. EMFORCED Framework

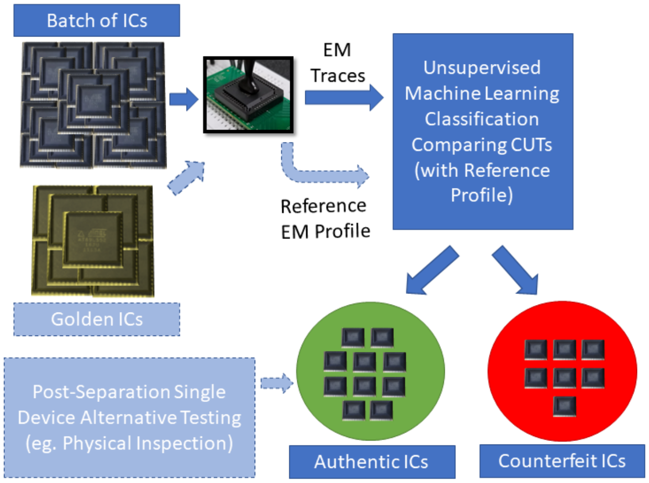

Fig. 1. EMFORCED Framework

Figure 1 shows EMFORCED's framework, in which, EM traces are obtained in a non-destructive and low-cost manner from suspect ICs without the need for test vector application or prior knowledge of the chip under authentication. Additionally, the traces are evaluated using unsupervised (label-free) machine learning methods and can be categorized by comparing with known-authentic traces from 'golden' ICs or post-separation alternative testing on a single IC from the groups. In this paper, we specifically demonstrate the effectiveness of EM-based measurements and subsequent fingerprinting for *remarked* and *cloned* IC detection. In order to emulate remarked and cloned ICs, we source chips with the same IP core (8051) from 3 vendors and distinguish between them without prior knowledge of the vendor labels. EM-based classification is not limited to these categories, as it can be extended to address other counterfeit IC threats as briefly discussed below.

- If the EM signature is able to capture foundry manufacturing traits across different designs, it can be used for foundry-of-origin identification.
- If EM traces can capture process variations from die-to-die, they can be readily used as PUFs in overproduction prevention protocols and chip authentication. Such PUFs would incur no overhead, as variation intricacies would be captured in the EM side-channel.
- EM traces can also be correlated with device operating frequency for the detection of recycled and remarked ICs. This would be based on the intuition that their operating frequency (and thus, EM emission fingerprint) would be degraded due to prior usage and harsh recycling processes.
- In our demonstration, we utilize digital ICs and EM emission from the stimulated clock tree. This can be extended to analog and mixed signal chips. When the chip is stimulated via any pin (e.g., power/ground) which causes significant current fluctuation, a distinct EM signature can be generated.
- Such stimulation and EM emission measurement techniques can also be extended to memory (e.g., SRAM, Flash) and FPGA chips, without the need for loading programs/input vectors and/or incorporating custom blocks into the design.

A. Threat Model

In our threat model, a customer who acquired a digital IC from the open market wants to verify whether the chip (or a batch of chips) is authentic and originated from a legitimate vendor, and whether the design underneath the package is the expected one. Depending on the types of chips available for reference and testing, we could encounter different scenarios.

1) A batch of known-authentic chips are available, whose EM traces are collected and profiled. Once a suspect chip (or batch of chips) is obtained, its

EM profile can be compared with that of known-authentic ones using similarity or distance measures (e.g., Euclidean distance). If the EM profiles are sufficiently different (or belong to a cluster that is not expected), the verifying party can be certain that the chip is counterfeit.

2) A batch of chips is obtained, of which many could potentially be remarked or cloned. However, the verifier does not know which chips are genuine and which ones are suspect. EM measurements are performed on all chips, and unsupervised machine learning (e.g., PCA) is performed on the EM traces. This should ideally lead to the formation of distinct clusters, after which, chips from within each group can be sampled from for further evaluation (e.g., physical inspection). This can assist in determining which clusters of chips are counterfeit and which are authentic.

In this paper, we address (2) as a case-study, where the classifier is given unlabeled EM traces from different 8051 designs (from different vendors), and is tasked with separating the traces into vendor-specific clusters. Once this is done, we use the proper vendor labels to calculate the classifier accuracy. Further, we specifically address the case of distinguishing between *different designs fabricated at the same or different foundries*. Distinguishing between the same ICs fabricated at different foundries (regardless of the underlying design) was the focus of the work in [8] and [18].

IV. Electromagnetic Emissions

It is widely known that electrical wires carrying a switching current generate EM waves. The strength of these emanations are directly proportional to (1) the frequency of the signal propagating through the wire, (2) the length of the wire, and (3) the magnitude of current carried by the wire. In a VLSI chip, unintentional EM emanations are considered a serious issue, as they can couple to nearby components and electronic systems, leading to malfunction. Various solutions, industry standards, and EM compatibility testing have also been developed to ensure EM emissions from chips and electronic systems (1) are properly attenuated within a specified distance, (2) do not contain spectral content outside the designated frequency band (ideally, higher frequency contents are suppressed) and (3) will not unintentionally interfere with nearby devices [19].

In a VLSI chip, the most significant source of these EM emanations is the clock tree network [20]. This stems from the elongated traces found in the clock distribution network, the fast transition time of the clock edges, its periodicity, and high frequency. Spectral analysis of the clock signal shows that energy is concentrated in narrow bands near the harmonic frequencies (with higher harmonics being the most problematic for electromagnetic interference (EMI)). The EM emissions tend to be maximized on the rising/falling clock edge. During a rising/falling edge, many components on the IC simultaneously switch and draw large amounts of current from the power distribution network (PDN), leading to simultaneous switching noise (SSN) [21]. This results in large EM emissions, as the PDN is the largest parasitic antenna structure on the IC layout. In fact, various techniques such as reduction of the clock rise/fall time, introducing clock skew, spread-spectrum clock signal generation, and inserting on/off chip decoupling capacitors have been proposed to counter EMI from the clock tree and ensure EMI-standard compliance [20].

In this work, we argue that such EM emanations (particularly the ones generated from a clock pulse and subsequent switching activity on the chip) can be used to generate a unique *design-specific signature*. This is because every design[2] has a unique clock distribution network associated with it. Placement of clock sinks (i.e., flip-flops) are different from one design layout to another and, therefore, clock tree synthesis tools create significantly different routing networks and buffer locations to minimize skew, wire-length, and delay in those designs. Equation 1 expresses the intensity of EM emissions (E) accumulated over the entire surface of the chip. When forming an EM-based fingerprint, the collected traces will be a complex summation of the currents propagating throughout the design. If the entire CUT area is represented as a X,Y grid of point sources, the measured result can be approximated by:

$$E \propto \int_y \int_x \frac{\vec{S}}{4\pi \vec{r}^2} dx\, dy = \int_y \int_x \frac{\left(I_{(x,y)}\right)^2 Z_{(x,y)}}{4\pi \left(r_{(x,y)}\right)^2} dx\, dy \tag{1}$$

Each of these positions requires a current (I) and complex load (Z) to determine the apparent power (S), in addition to the distance from the observation point (r). Note that this approximation does not directly address the medium through which these waves are propagating (such as the silicon and packaging materials), which can be factored in using permittivity constants if needed.

[2] Here, design refers to the IC layout

This relationship gives insights into the EMI occurring within the measurement environment, giving meaning to not only the characteristics of the input waveform, but also the relative measurement position over the die. The EM profiles from clock trees of two different designs are expected to be different (*inter-design variability*), due to the complex network of die-level emitters as described in Equation 1. However, for a reliable ‘fingerprint’, we also require low *intra-design variability*. This requires two chips/dies containing the same design (i.e., identical clock tree) to produce consistent signatures within a certain margin (e.g., due to process variations). This differentiates fingerprints from PUFs, in that PUFs require unique signatures from the same layout in two or more different chips.

V. EMFORCED Fingerprint Extraction

Our approach utilizes the previously discussed physical properties of ICs to extract a design-specific fingerprint for a given fabricated design. The completed setup consists of a function generator (to generate the clock pulse), power supply (5V), a mixed signal oscilloscope (MSO), a near-field EM probe and holder, a high bandwidth amplifier connected to the EM probe output, and an interfacing board to mount the CUT. The entire EMFORCED setup is shown in Figure 2.

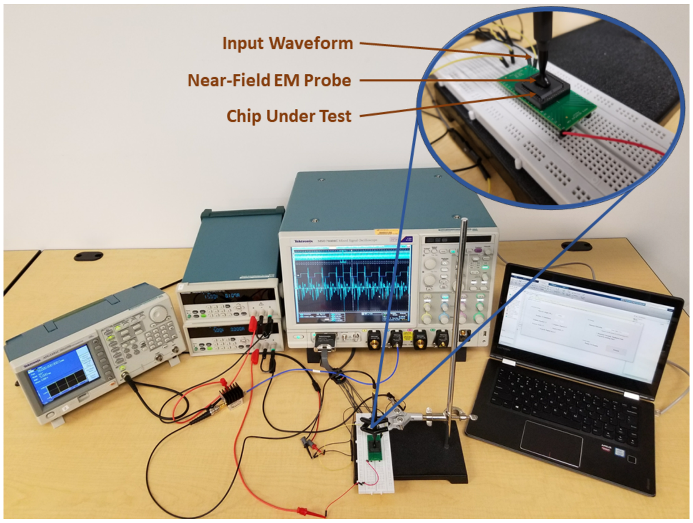

Fig. 2. Experimental setup for EMFORCED fingerprint extraction.

A. Overview of Experiments

For our fingerprinting experiments, 8051 microcontroller ICs were selected from 3 different vendors: Atmel, Maxim, and NXP. Ten of each of these devices were purchased through a single retailer. These ICs were specifically selected, because they had very similar functional characteristics, (e.g. instruction set architecture, operating voltage, and package type) while also being readily available for purchase. Since they were all purchased through a single retailer in one transaction, all of the devices had the same characteristic markings and there is likely no variation in fabrication lots, dates or packaging location within a given vendor set. Obtaining chips with various date and lot codes would have been preferred. Unfortunately, such information can only be received after purchase, which makes it hard to order a batch with varying date/lot codes. All CUTs are assumed to contain the same 8051 IP core and are housed within a 44-PLCC package [22]. Specific device fabrication facility and technology node are not known, as they are not openly provided by the devices’ supporting documentation. Estimation of these parameters is beyond the scope of this paper, although we believe this information may potentially be recovered from similar EM-based measurement techniques.

The experimental measurements were taken using an amplified near-field EM probe and external clock input. The probe used in this experiment was factory-tuned to collect radiated fields from a single direction and suppress perpendicular fields [23]. This helps to suppress noise from external sources such as PCB wiring, board-level jumper cables, and nearby equipment, alleviating the need for additional EM shielding around the setup. Given this unshielded, manually operated testing environment, additional variation will be present in the results. This may diminish the requirement for ICs from different date and lot codes in our experimentation. To collect EM emissions from the CUT, a 5V peak-to-peak square wave with 50% duty cycle was applied to enable observation of current settling from forced high speed transitions. This signal was output from a dedicated function generator at 16 MHz to comply with the 8051 devices’ typical operation frequencies. The devices were powered on by a 5V input from a programmable power supply, to ensure that all clock buffers were activated and that the supplied signals could fully propagate through the circuit.

Note that our experimental setup only requires a clock pulse and does not need any programs or specific input vectors to be loaded, which makes it practical for black-box analysis of COTS components, whose functions are usually not fully known. Further, physical modification of the die or packaging is not required. It could also prove useful for one-time-programmable (OTP) chips, on which specific test programs for fingerprinting cannot be loaded. We also point out that the measurements discussed here should not damage the original functionality or reliability of the devices. This is because the clock signal we applied is exactly at the specified frequency, and the time to collect the EM emissions (manually for 10 acquisitions) was less than two minutes (plus, input vectors are not applied, due to which, switching activity in the logic and thus, aging, is minimal). The total collection window per acquisition was set as 10 microseconds to in accordance with the MSO's maximum sampling frequency of 25 GS/s and to observe traces over several clock cycles. It should be noted that this method is in no way restricted to the specific instrumentation used in our lab, although for optimal results and scalability, real-world solutions should attempt to limit the differences between measurement environments for the most consistent results.

B. Principal Component Analysis Method and Implementation

Principal Component Analysis (PCA) is a very powerful and popular technique used for dimensionality reduction as well as feature extraction [24]. The basis behind PCA is to convert possibly correlated variables into a set that is linearly uncorrelated (referred to as principal components). These principal components represent the data in a manner which highlights the most expressive features of the signal by projecting the data in orthogonal directions that contain the most variance. Where the first principal component represents the projection of the data with the most variance, the second principal component represents the second most, and so forth. Furthermore, the number of distinct principal components in a data set will be the smaller of the number of observations or original variables. By determining which principal components contain the most variance, one is able to quantify the importance of each dimension of the data and provide a reasonable characterization within a reduced dimensional space. In our analysis, PCA is used to reduce the 250,000 samples-per-measurement feature vector down to a dimensionality of 44. This is the number of measurements used for training (45) minus one.

VI. Experimental Results & Discussion

Figure 3 below shows the small variations between individual measurements of Atmel devices (*intra-vendor variations*). These variations are an accumulation of differences in die fabrication, packaging, relative probe positioning resolution, and variations in the external clock input signal. It should be noted that all device positioning was done by hand without the assistance of an automatic or programmable stage, which would have provided more precise positioning. Automating and calibrating this portion of the setup process should provide even better results between each of the intra-vendor datasets. EM measurements heavily depend on the ability to recreate the same measurement environment including relative alignment between the CUT and EM probe as well as the external fields which may have influenced the readings.

Measurements were taken for each of the 30 devices (3 vendors × 10 ICs each) and similar variations occurred within the NXP and Maxim groups as seen from the Atmel devices. The *inter-vendor variations* can be observed in Figure 4. These differences can be attributed to fabrication differences in the power networks, clock distribution routing (major contributor), decoupling capacitors, and transistors, all without decapping or physically modifying the IC.

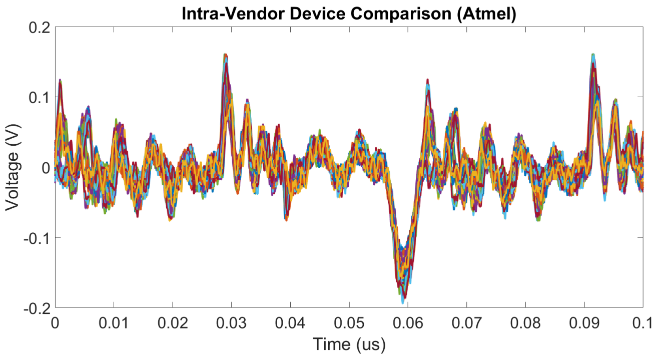

Fig. 3. Time-Domain plot showing intra-vendor variability from Atmel device data.

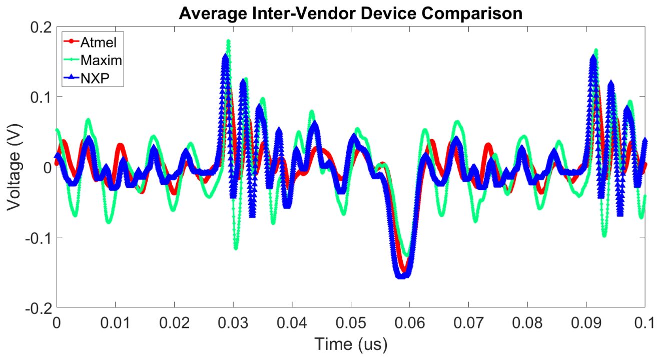

Fig. 4. Time-Domain plot of average design-specific fingerprints from each vendor.

A. Utilizing Second External Clock Pin

The 8051's each have two external clock pins. As such, the measurements previously described were replicated for the second external clock signal. Since the two clocks pins endure different input loading effects and thus, different RLC characteristics, we assume that the signals can be characterized as two separate fingerprints. Utilization of the two clock pins is equivalent to doubling the number of devices in our experiment. This helps generate additional features which can be used for more robust classification of a specific IC (see Table I).

	Domain	Accuracy		
		Euclidean	Minkowski	City Block
Clock Pin 1	Time	99.21%	99.32%	99.21%
	Frequency	100%	100%	100%
Clock Pin 2	Time	99.68%	99.68%	99.68%
	Frequency	99.97%	100%	99.97%

TABLE I
PCA CLASSIFICATION ACCURACY

B. Machine Learning

The collected time-series EM data was processed primarily using principal component analysis (PCA), which allowed us to reduce the dimensionality of the data-set from the total number of sample points (250,000) to 44. To train our model, 5 ICs were randomly selected from each vendor and 3 measurements were randomly chosen from each of these 5 devices, in order to cross-validate our results and remove any selection bias. For each set of 30 CUT's, 15% of the 300 total measurements were used as training data and the remaining 85% was used as test data. Accuracy metrics were calculated by averaging 100 executions of PCA. To perform the CUT-vendor classification, 3 different distance metrics were used per trial; Euclidean, Minkowski, and City block. The averaged values are shown in Table I for both the first and second external clock input measurements. Although most previous EM techniques utilize analysis in the frequency-domain, visibly distinguishable features existed within the time-domain data with minimal deviation between intra-vendor collections. Therefore, we opted to analyze the time-series data in addition to the transformed frequency data. The plot in Figure 5 shows the EM data forming distinct clusters. The separation of these clusters (comprised of the PCA projected EM data across the first 3 principal components), demonstrates clear distinguishability between designs.

C. Attack Resilience Analysis

The primary goal of an attacker would be to replicate the EM signature on a design of his or her choosing. As our design fingerprinting technique enables the verifying party to gain insights into the inner workings of the CUT, the attacker would be required to emulate the complex RLC network responsible for modulating the input waveform. He or she would likely need to have substantial assets to not only fabricate the malicious design, but also attempt to estimate the effects of a complex network on EM emissions with temporal and spatial resolution. Modern EM-based simulation tools lack the ability to estimate complex model structures with spatial accuracy while keeping in mind the larger effects of the surrounding network. Most EM approximation methods rely upon either utilizing the physical parameters of a single fundamental device (e.g., a single transistor) for nano-scale experiments or, through circuit simulation, calculating the total switching to extract information from crypto-cores. These methods will not be successful in generating an accurate EM profile of a given design, as simulations based on physical parameter testing are not scalable at this time. Should an attacker gain access to a simulation tool with this capability, they would be required to modify their circuit's placement and routing constraints to comply with the desired fingerprint, which, for more complex circuits, could be nearly impossible. If the attacker was able to create an effective model and an accurate cloned signature when probed from the center of the die, the fabricated version of the device may still not reproduce the same fingerprint, depending upon foundry-specific variations and packaging constraints.

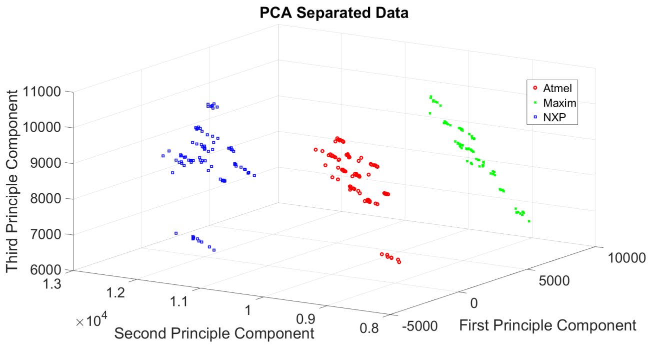

Fig. 5. A 3-D plot for visualization of the post-separation experimental data.

It should be noted that there are certain limitations to the robustness of our approach. For example, the resolution of the near-field EM probe and measurement equipment provides an inherent "tolerance" within the measurement environment, which could deem an authentic and counterfeit IC as the same should they be within a certain threshold. Manufacturing variations and spatial

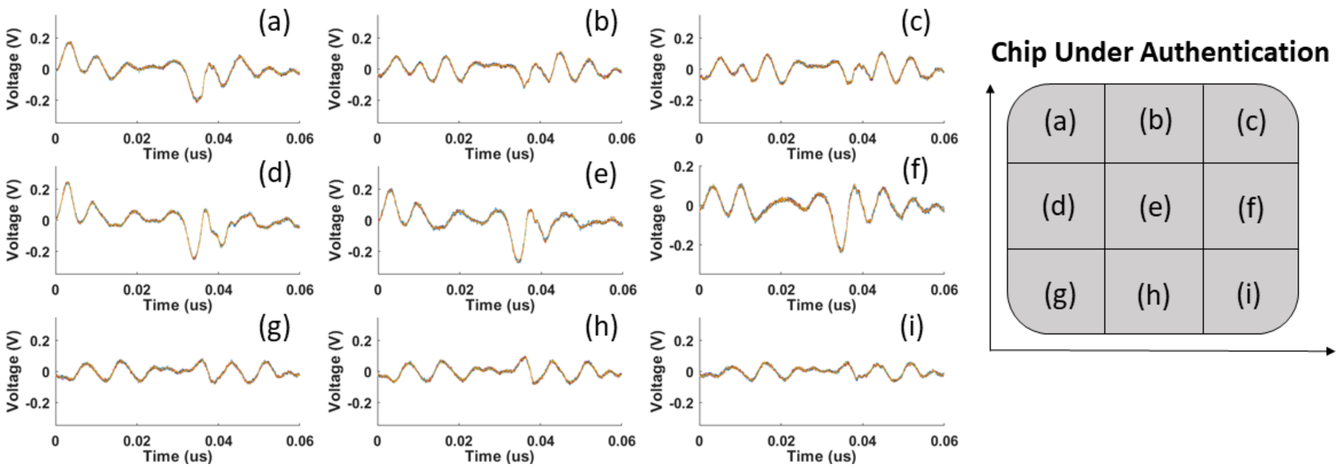

Fig. 6. A coarse sample of the numerous EM fingerprints available through changing the location of the probe relative to the die. Die positioning is shown with labels (a)-(i).

resolution of the probe further expand this tolerance. An attacker could potentially use this tolerance to create a cloned signature that conforms to these metrics. We note that the use of a programmable stage that allows accurate positioning of the probe and reduction of measurement-to-measurement variation should reduce this vulnerability by providing tighter bounds on the classification.

VII. Multi-Parameter Counterfeit Detection

Thus far, our experimentation has focused exclusively on identifying a given device by using a single parameter. Here, we explore the potential of introducing multi-parameter testing and provide insights into how this could maintain high classification accuracy while expanding the number of IC types. The tests discussed below focus on EM-based approaches, but combining EM with another measurement, such as power analysis or optical inspection, is also possible.

A. *Exploiting Spatial Probing Parameters*

In the approach described in the previous section, all measurements were taken from the center of the CUT. This was done to maximize the EM response collected from the die itself. In order to study the impact of probe location on the CUT, we measured EM emission from various regions on the IC package. The results from Figure 6 clearly show that EM measurements vary between different locations. In the future, we plan to devise fingerprinting schemes that collate measurements from various locations, instead of just the center. This simple extension would provide another degree of difficulty for an attacker. While attempting to simulate/clone the EM fingerprint, they would now be required to incorporate the spatial location of the measurement probe in addition to the on-chip EM radiative grid itself.

B. *Measurement Distance Accuracy*

Having explored the X,Y plane on the surface of the CUT, we sought to determine whether modifying the proximity of the probe to the surface, or Z-axis, provided any additional information. Changing the probe's vertical location relative to the chip surface is not ideal for extracting circuit switching noise for applications such as crypto-key extraction (since we desire the highest signal-to-noise ratio). However, since our technique is targeted at extracting a design-specific signature, we are able to see added physical effects from slightly farther-field measurements. Figure 7 shows how the signal changes when measuring EM with a near-field probe while introducing a separation distance. Modification of the probe height allows for the radiation to travel a bit further. This would allow the wave to interfere with itself to create new information, similar to what was seen in the X,Y plane (see Figure 6).

To determine the potential effectiveness of varying the probe proximity, the normalized maximum cross-correlation between signals obtained at different heights was calculated for an Atmel device. In Figure 8, the red Atmel line shows the cross-correlation between an Atmel measurement while contacting the device (i.e. a separation distance of 0mm) and at varying distances. For the low separation values with high cross-correlation, this implies confidence in the measurement environment, i.e., even with a small height variation, the classification results should remain the same. Upon moving further away from the device, (below $\approx 90\%$ cross-correlation or $\approx 2mm$), the collected waveforms should contain adequately new information to be introduced into the analysis. The green and blue lines provide insights into the similarity between the Atmel measurements at a given distance when compared to the Maxim and NXP responses on contact. Notice that at every separation distance, the cross-correlation between the Atmel device and the other vendors remains fairly consistent. This shows that the waveforms collected from measuring at a distance provide additional information that not only deviates from the intra-vendor measurements, but also maintains a considerable uniqueness in inter-vendor comparisons.

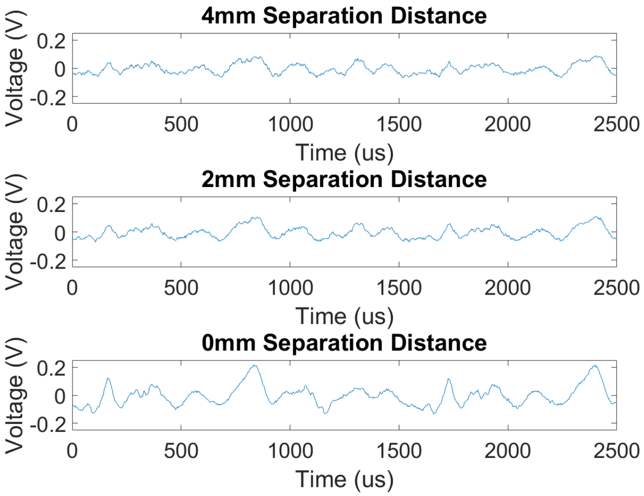

Fig. 7. Normalized maximum cross-correlation between near-field measurements taken with various input voltages.

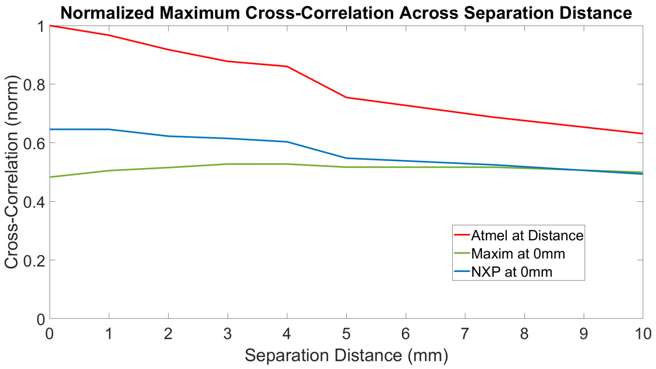

Fig. 8. Normalized maximum cross-correlation between measurements from various distances from the device under test.

C. Input Voltage Variation

While testing the ICs, we attempted to maintain typical operating conditions so-as not to damage the CUT. We applied various input voltages ranging from three to five volts peak-to-peak for the clock signal input. Variation of signal magnitude could provide another dimension of interest when discussing multi-parameter analysis. However, we cannot recommend utilizing out-of-spec voltages on parts which are intended for use in a system. This method would likely be carried out in a post-separation single device alternative test to increase confidence in characterization while maintaining low cost. Figure 9 shows a similar comparison as Figure 8, with the cross-correlation between Atmel devices across a range of voltages and the specific vendor at five volts. The cross-correlation within this voltage range seems to be slightly higher than that seen from the distance analysis, although the same trend of uniqueness among both intra and inter-vendor is apparent. As we do not have access to information regarding the die-level operating voltage or the surrounding voltage regulators and level shifters, it is difficult to identify the physical parameters which could be introducing this deviation. The CUT was not designed to accept an input voltage less than 4.5V, so we assume that the more steep drop off in cross-correlation, shown in the red Atmel line between 3.5V and 4.5V, may be attributed to this.

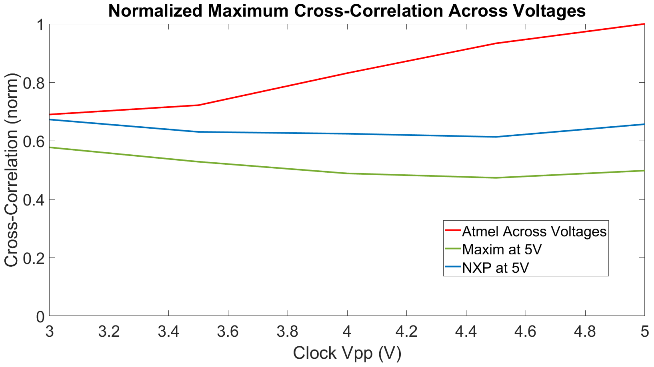

Fig. 9. Normalized maximum cross-correlation between near-field measurements taken with various input voltages.

VIII. Future Work

In the future, we plan to increase the robustness of EM-based counterfeit detection by:

- Introducing a more comprehensive sample space: The addition of ICs with various date and lot codes, and collecting information from several new types of ICs would benefit the confidence of EM-based counterfeit detection.
- Improving measurement environment reliability: Introducing an automated testing environment which utilizes a programmable translation stage and provides added EM shielding from external signals

would ease measurement replication and tighten the PCA groupings(i.e. further improve classification).

- Gaining additional insights into the relevant physical phenomena: The presented methodology effectively extracts analog device parameters from a digital circuit. Further exploring the relationship between measured EM emissions and the underlying physical parameters may lead to combating new problems and reducing the need for golden information by providing a deeper physical understanding of the CUT.

IX. Conclusion

We believe that EM-based fingerprinting offers a fast, low-cost, one-size-fits-all approach for detecting several types of counterfeit ICs. In our case study on remarked and cloned ICs, our experimental results and PCA-based unsupervised machine learning yielded an average accuracy of more than 99% across different vendor groups. We observed well-separated clusters for EM traces from different vendors for the same IP core, indicating that EM measurements are well-suited for design fingerprinting. While we limited our demonstration to digital ICs, the same technique could also be extended to analog and mixed signal ICs, potentially with a different input stimulus (since clocks are rare in analog designs). In the future, we plan to develop a more robust testing environment and demonstrate our experiment-based EM-FORCED framework on other types of counterfeits, such as recycled and overproduced ICs.

References

[1] U. Guin, K. Huang, D. DiMase, J. M. Carulli, M. Tehranipoor, and Y. Makris. Counterfeit integrated circuits: A rising threat in the global semiconductor supply chain. *Proceedings of the IEEE*, 102(8):1207–1228, Aug 2014.

[2] U. Guin, D. DiMase, and M. Tehranipoor. Counterfeit integrated circuits: detection, avoidance, and the challenges ahead. *Journal of Electronic Testing*, 30(1):9–23, 2014.

[3] M. Tehranipoor, U. Guin, and D. Forte. Counterfeit integrated circuits. In *Counterfeit Integrated Circuits*, pages 15–36. Springer, 2015.

[4] U. Guin, D. Forte, and M. Tehranipoor. Anti-counterfeit techniques: from design to resign. In *Microprocessor Test and Verification (MTV), 2013 14th International Workshop on*, pages 89–94. IEEE, 2013.

[5] M. Miller, J. Meraglia, and J. Hayward. Traceability in the age of globalization: a proposal for a marking protocol to assure authenticity of electronic parts. Technical report, SAE Technical Paper, 2012.

[6] G. Suh and S. Devadas. Physical unclonable functions for device authentication and secret key generation. In *Proceedings of the 44th Annual Design Automation Conference*, DAC '07, pages 9–14, New York, NY, USA, 2007. ACM.

[7] B. Gassend, D. Clarke, M. Van Dijk, and S. Devadas. Silicon physical random functions. In *Proceedings of the 9th ACM conference on Computer and communications security*, pages 148–160. ACM, 2002.

[8] A. Ahmadi, M. Bidmeshki, A. Nahar, B. Orr, M. Pas, and Y. Makris. A machine learning approach to fab-of-origin attestation. In *Computer-Aided Design (ICCAD), 2016 IEEE/ACM International Conference on*, pages 1–6. IEEE, 2016.

[9] U. Guin, X. Zhang, D. Forte, and M. Tehranipoor. Low-cost on-chip structures for combating die and ic recycling. In *Proceedings of the 51st Annual Design Automation Conference*, DAC '14, pages 87:1–87:6, New York, NY, USA, 2014. ACM.

[10] Z. Guo, M. Rahman, M. Tehranipoor, and D. Forte. A zero-cost approach to detect recycled soc chips using embedded sram. In *Hardware Oriented Security and Trust (HOST), 2016 IEEE International Symposium on*, pages 191–196. IEEE, 2016.

[11] M. Alam, M. Tehranipoor, and D. Forte. Recycled fpga detection using exhaustive lut path delay characterization. In *Test Conference (ITC), 2016 IEEE International*, pages 1–10. IEEE, 2016.

[12] Z. Guo, X. Xu, M. Tehranipoor, and D. Forte. Ffd: A framework for fake flash detection. In *Proceedings of the 54th Annual Design Automation Conference 2017*, page 8. ACM, 2017.

[13] H. Huang, A. Boyer, and S. Dhia. Electronic counterfeit detection based on the measurement of electromagnetic fingerprint. *Microelectronics Reliability*, 55(9):2050–2054, 2015.

[14] O. Soll, T. Korak, M. Muehlberghuber, and M. Hutter. Em-based detection of hardware trojans on fpgas. In *Hardware-Oriented Security and Trust (HOST), 2014 IEEE International Symposium on*, pages 84–87. IEEE, 2014.

[15] N. Sehatbakhsh, A. Nazari, A. Zajic, and M. Prvulovic. Spectral profiling: Observer-effect-free profiling by monitoring em emanations. In *Microarchitecture (MICRO), 2016 49th Annual IEEE/ACM International Symposium on*, pages 1–11. IEEE, 2016.

[16] A. Lakshminarasimhan. Electromagnetic side-channel analysis for hardware and software watermarking. *UMass masters Thesis*, 2011.

[17] D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi. *The EM Side—Channel(s)*, pages 29–45. Springer Berlin Heidelberg, Berlin, Heidelberg, 2003.

[18] R. Helinski, E. Cole, G. Robertson, J. Woodbridge, and L. Pierson. Electronic forensic techniques for manufacturer attribution. In *Hardware Oriented Security and Trust (HOST), 2016 IEEE International Symposium on*, pages 139–144. IEEE, 2016.

[19] M. Ramdani, E. Sicard, A. Boyer, S. Dhia, J. Whalen, T. Hubing, M. Coenen, and O. Wada. The electromagnetic compatibility of integrated circuitspast, present, and future. *IEEE Transactions on Electromagnetic Compatibility*, 51(1):78–100, 2009.

[20] D. Pandini, G. Repetto, and V. Sinisi. Clock-tree synthesis for low-emi design. *Journal of Embedded Computing*, 3(3):197–207, 2009.

[21] Y. Villavicencio, F. Musolino, and F. Fiori. Electrical model of microcontrollers for the prediction of electromagnetic emissions. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 19(7):1205–1217, 2011.

[22] Atmel. *8-bit Low-Voltage Microcontroller*. Rev. 2601C.

[23] Langer EMV-Technik. *Passive RF Near-Field Probe*. Rev. 1.

[24] J. Shlens. A tutorial on principal component analysis. *CoRR*, abs/1404.1100, 2014.