IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 6 September 2022, accepted 7 November 2022, date of publication 21 November 2022,
date of current version 30 November 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3223998

RESEARCH ARTICLE

Circuit Activity Fingerprinting Using Electromagnetic Side-Channel Sensing and Digital Circuit Simulations

ANDREW S. KACMARCIK[1], (Student Member, IEEE), PRATEEK JUYAL[1], (Member, IEEE), MILOS PRVULOVIC[2], (Senior Member, IEEE), AND ALENKA ZAJIĆ[1], (Senior Member, IEEE)
[1]School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA 30332, USA
[2]School of Computer Science, Georgia Institute of Technology, Atlanta, GA 30332, USA

Corresponding author: Andrew S. Kacmarcik (akacmarcik3@gatech.edu)

This work was supported in part by the Office of Naval Research (ONR) under Grant N00014-17-1-2540.

ABSTRACT This paper introduces a novel circuit identification method based on ''fingerprints'' of periodic circuit activity that does not rely on any circuit-specific reference measurements. We capture these ''fingerprints'', consisting of fifty harmonics of the circuit activity, using digital circuit simulations and near-field measurements of the EM backscattering side-channel. Utilizing a novel technique and algorithm, we augment our measurements, removing sources of noise and other irregularities not present in the simulation, in order to relate an unknown circuit measurement with a known circuit simulation. A matching threshold of less than 1 dB difference between the simulated and measured fingerprints is set, and the matching performance is evaluated across multiple hardware instances exhibiting a strong resistance to false positives. Using various match statistics, decisions on the circuit identity can be made based on the simulated and measured fingerprint pair with the best matching performance. The results show that we can identify fingerprints of digital circuits with up to 95% accuracy using the proposed method.

INDEX TERMS Electromagnetic transients simulation, experimental measurement, fingerprinting analysis, hardware security, harmonic analysis, integrated circuits, remote sensing, software modeling.

I. INTRODUCTION

Identification of circuits through digital fingerprinting has been demonstrated with a variety of techniques in literature including the fingerprinting of path-delays within an integrated circuit (IC) [1], IC magnetic fields [2], [3], [4], [5], and electromagnetic (EM) side-channels [6], [7], [8], [9], [10], [11]. These identification techniques can provide device authentication [12], [13], [14], [15], [16], device tracking [17], [18], [19], and counterfeit detection [4], [7], [11], [20], [21]. Traditionally, authenticating an IC's identity required invasive techniques to verify the physical circuitry, either leaving the device in an inoperable state [22], or ''semi-destroyed'' but still operational [9]. In contrast, side-channel research has provided non-invasive and non-destructive techniques for authenticating an IC that do not adversely affect the operation of the device [10], [23]. Utilizing the EM side-channel requires no physical contact with, or invasive modifications to, a Device-under-Test (DuT), however it is not without its limitations. Measurements of unintended EM emanations are, by their nature of being unintended, extremely weak and susceptible to noise. By applying a strong source frequency to the surface of a DuT and receiving the reflections, a method known as backscattering, the signal to noise ratio (SNR) of the EM side-channel can be improved [10], [24], [25], [26]. An additional benefit of backscattering for circuit fingerprinting is that the reflected power contains not only modulated circuit activity, but also reflections of characteristic impedances from dormant portions of the DuT. The EM backscattering side-channel

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

exploits the switching impedance states of transistors within a circuit to mix and up-shift the circuit activity to the frequency of an incident carrier.

Another limitation of the EM-side channel is its sensitivity to change in the measurement environment, meaning capturing consistent results is a challenge. Historically, measurement of these side-channels required ''Golden Circuit'' or ''Golden Chip'' reference measurements in order to differentiate between experimental measurements of circuit designs [4], [7], [11]. A ''Golden Chip'' is any integrated circuit that is guaranteed to have been manufactured without any tampering or deviation from the original design. For many of the largest semiconductor manufacturers however, creating a ''Golden Chip'' is not possible, as the industry practice is to design integrated circuits ''in-house'' with domestic labor, but use foreign labor and equipment in order to fabricate those circuits. There are examples in literature of ''Golden Chip''-free circuit identification using measurements of trusted on-board components [27], [28], routing or timing statistics [23], [29], [30], thermal imaging [31], machine learning [32], and even brain-inspired detection architectures [33], but these techniques have their own limitations. Most of them require some measurement control training period on what is essentially a ''Golden Chip'', and those that do not, only demonstrate a method of clustering, lacking decisions on circuit identity. Unlike ''Golden Chip'' based methods, where changes in the measurement environment mean needing to re-establish the control by re-measuring the ''Golden Chip'', a simulation is constant and only needs to be performed once for a specific circuit design.

In this paper, we propose a novel method allowing for comparing and relating simulated and measured circuit activity that can be applied to a number of applications. For instance, using simulations as a reference, identifying circuits would require only one measurement of the unknown device, which could then be compared analytically to any number of simulated fingerprints. While each simulated circuit in this study was designed identically to the measured hardware implementation, to account for the multitude of environmental factors and losses present only in the measurements, we propose a novel, circuit-independent, calibration technique and measurement variation algorithm enabling the matching of measured and simulated fingerprints within 1 dB. In fact, we show not only the ability to match measured and simulated fingerprints from the same circuit with up to 95% accuracy, but also a strong resistance to false-positives involving similar circuit designs through multiple match statistics verified across multiple hardware instances. With this in mind, the main contributions of this work are the following:

- A non-invasive frequency-independent profiling and IC activity fingerprinting method, based on sensing electromagnetic side-channels.
- A highly efficient and simple methodology to match backscattered electromagnetic side-channel emanations of circuit activity both measured experimentally and verified through RF circuit simulation.
- A device-agnostic method for achieving higher measurement accuracy by accounting for experimental variation and noise.

The rest of this paper is organized as follows. Section II discusses the circuit activity captured, details information about the measurement environment, and provides specifications on the measurement setup and data collection processes used. Section III discusses the proposed matching technique by detailing the steps taken to develop the procedure and major algorithm. Section IV shows results for both the simulated and measured circuits, and the matching method performance on those circuits is discussed. Finally, conclusions are presented in Section V.

II. SIDE-CHANNEL SENSING

A. BACKSCATTERED HARMONIC MEASUREMENTS

While small changes to a circuit design are not usually detectable, they do affect the operation of the circuit. Specifically, additional circuit paths manifest as very short changes to the overall time domain switching behavior of the transistors used. The net result of a single inverter switching states produces a minute change, but in a chip with millions of transistors switching states during operation, the effect becomes measurable [34], [35]. Unlike the change in current that occurs during transistor switching, these changes in impedance remain for the entire clock period. Since any on-board clocks have to be generated through an oscillator of some kind, no matter what digital logic is happening within the circuit, it is tied to an analog source. When analog frequencies are generated, harmonic multiples are produced. These harmonics represent small time changes in the generation of a frequency, proportional to the reciprocal of the harmonic number. For example, the first harmonic represents activity over an entire period, the second harmonic represents only activity over the first half of the period, the tenth harmonic represents one-tenth of the period, and so on. We use higher order harmonics because most circuit activity occurs immediately after the clock edge, allowing us to have a finer temporal resolution and detect changes resulting from only hundreds out of the total millions of transistors within the Field Programmable Gate Array (FPGA) used for the hardware implementation of our circuits.

In past work [10], only the first 35 harmonics were used. Here, we extend our measurements out to 50 harmonics of the master clock frequency, 50 MHz for the Altera Cyclone V DE0-Nano FPGA, to reduce our temporal resolution to 0.4 ns. While the backscattering process creates harmonics both above and below the carrier frequency, we choose to only measure the upper sideband mixing products because of the impact of interference on the lower sideband mixing products from common low frequency bands such as the 2.4 GHz Wi-Fi band. Since the magnitude of the experimentally received power of a harmonic will be different compared to a simulation, we compensate by calculating the harmonic

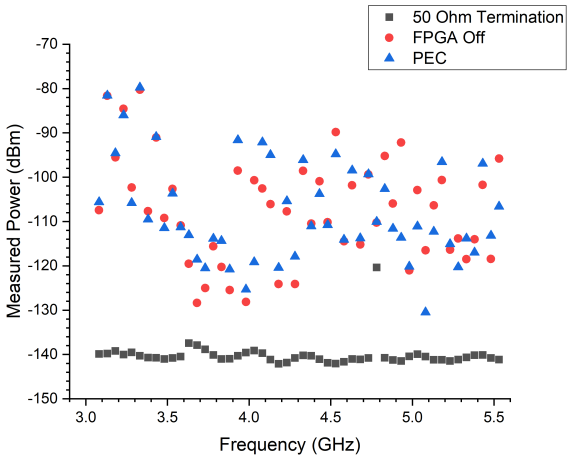


FIGURE 1. Measured power of clean plates.

ratio for the received power and use those values to compare the experimental results to the simulated results. The term *harmonic ratio* in this paper refers to the difference between the received power for harmonic h_n and that of harmonic h_{n+1}. This does mean that our 50 data points is reduced to 49 data points but it also allows us to characterize a circuit's activity based more on the relative envelope of the harmonics rather than their magnitude. However, these ratios are calculated using the assumption that each measurement point is relative to the same fixed reference. In the simulation this is true, and in experimental measurements, this fixed reference is the noise floor.

B. CLEAN PLATE CHARACTERIZATION

Several measurements were taken in order to remove environmental noise from our measurements, bringing them closer to our ideal simulations. This was accomplished by means of "Clean Plate" measurements, where "Clean Plate" refers to the idea of a calibration measurement meant to establish a baseline of the measurement environment absent a DuT. The first "Clean Plate" measurement was taken to calibrate the noise floor of our Keysight N9030B spectrum analyzer. As one can see in Fig. 1, the *50 Ohm Termination* plot of our instrument's noise floor is not flat, and in fact exhibits a large increase in received power from harmonic 11 to 12 near 3.6 GHz. Accounting for these errors is important because if the measured circuit activity at harmonic 11 has a slightly greater received power than that at harmonic 12, then the ratio of the two harmonics should be positive. However, since the instrument has a large jump in its reference at harmonic 12, the result could be that harmonic 11 is measured to have less power than harmonic 12, leading to an incorrect negative harmonic ratio. In addition to measuring the noise floor of our instrument, we also took "Clean Plate" measurements to see the effect of our probe [24] on our measurement setup, the first being the probe's response with no DuT present. By measuring the received backscattered power from the probe positioned above an electromagnetically reflective surface, in this case a block of aluminum, we were able to approximate the frequency response of our probe. For this measurement, seen in Fig. 1 as *PEC*, the amplifier, cables, and position of the probe used in all other measurements was kept constant. The final clean plate measurement was taken to identify the backscattering loss of a dormant DuT. While the other two measurements are dependent on our measurement setup only, this final "Clean Plate" will change depending on the DuT measured. We measured the received backscattered power when the FPGA was disconnected from power in order to determine how much power was absorbed into the chip package, versus the power reflected by the physical structure of the chip without any circuit activity. The results of that measurement when averaged across the chip surface can be seen in Fig. 1 as *FPGA Off*. When compared with actual measured circuit activity, there is an approximately 20 dB increase in the received backscattered power from the FPGA off to the FPGA on. While the results of each clean plate measurement deserve further research, in this study we utilized only the PEC and 50 Ohm measurements to calibrate our circuit measurements. As discussed in Section III, we first correct the PEC measurement using the difference from the 50 Ohm measurement, then augment our measured circuit activity with this "corrected" PEC measurement. Since we are interested in harmonic ratios, harmonic differences from the measured circuit activity and the corrected PEC measurement are performed resulting in "augmented" experimental harmonics. In the next section, we will detail the measurement setup and procedure used to capture the backscattered harmonics of circuit activity.

C. MEASUREMENT SETUP

The experimental setup has been illustrated in Fig. 2(a), along with a labeled top-down image in Fig. 2(b) of our custom EM probe [24] with separate E-Field and H-Field sensors. To perform backscattered measurements, we first apply a +15 dBm E-field at 3.031 GHz created by a Keysight N5183A Signal Generator to an Altera Cyclone V FPGA. The backscattered H-field is received by the probe, developed in [24], and amplified by a Pasternack PE15A1010 40 dB LNA before being measured by a Keysight N9030B Spectrum Analyzer (SA). The Altera Cyclone V SoC, Fig. 3(a), is packaged on a Terrasic evaluation board mounted onto two perpendicular Zaber Technologies X-LSQ150B linear motion stages. The EM probe's position is fixed 1 mm above the top left-hand corner of the FPGA die where its near-field resolution is only 1 mm. This distance was chosen in order to maximize the received power while remaining out of contact with the DuT. During testing the motion stages move the board 1mm at a time traversing each column in the +X direction for every row in the −Y direction through a 225 mm^2 area shown in Fig. 3(b). At each position, the board is programmed using Intel Quartus Prime and Verilog files developed by the authors for each circuit being measured. Since programming occurs at each position, the impact on the results of the order in which the measurements were captured

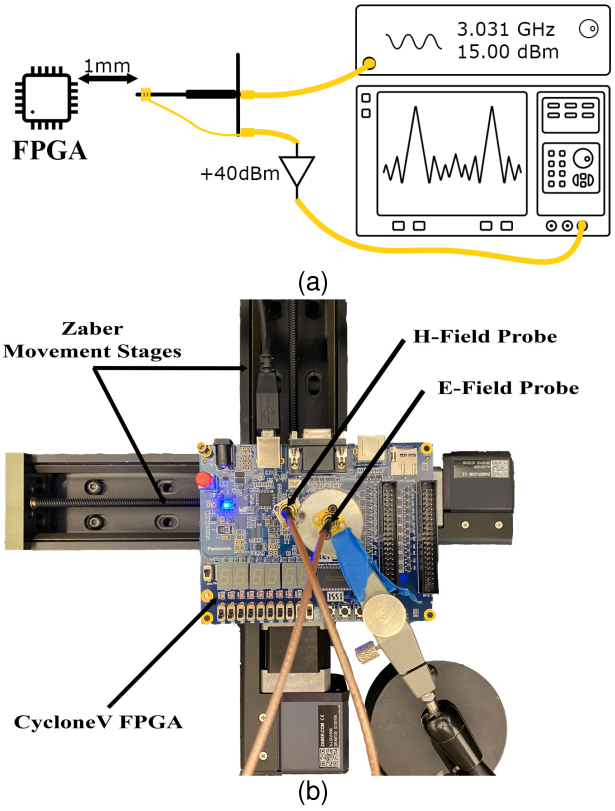


FIGURE 2. Backscatter measurement setup (a) diagram and (b) picture.

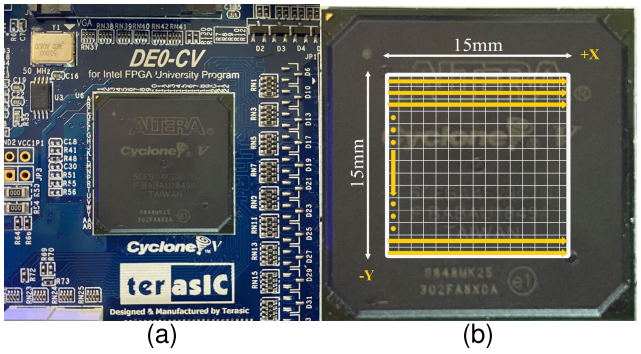


FIGURE 3. (a) Cyclone V FPGA, and (b) FPGA measurement area.

is minimized. After being programmed, the SA, using a 1 Hz resolution bandwidth, returns the frequency and power of the highest peak within a 4 kHz range centered on each harmonic.

To account for environmental variations, we measure 50 harmonics ten consecutive times at each position. Additionally, to ensure that measurements are independent of circuit run-time, the FPGA is re-programmed after each round of 50 harmonic measurements. This process is controlled entirely via a MATLAB script that stores data from the SA within 5-dimensional matrices (scan number, harmonic, program, x position, y position) for later analysis. Results of the measurements will be discussed in Section IV. Each circuit design was chosen for its ability to be implemented not only on an FPGA, but also in circuit simulation software,

TABLE 1. Measured variation for harmonics of circuit activity.

Circuit	Min [dB]	Max [dB]	Mean [dB]
Twenty Inverters	9.2 @ H6	49.2 @ H20	27.1
Four Bit Counter	7.7 @ H6	50.1 @ H49	27.9
AES Abstraction	5.8 @ H6	48.1 @ H48	28.6

specifically Ansys Electronics Desktop (EDT). We propose that corporate IC designers with questionable fabrication facilities would have no problem performing accurate circuit simulations of their designs before sending them to be manufactured, and that any design would utilize $> 50\%$ of the resources available. As discussed in [36], when using the EM backscattering side-channel, the greater number of transistors utilized in a design, the greater the backscattered power from circuit switching activity. However, it was difficult identifying circuit designs that could be simulated in a reasonable time frame while also utilizing enough FPGA resources to be detectable. Simulating a functional circuit large enough to utilize $> 50\%$ of the resources of our FGPA was not feasible, and simple circuit designs utilized $<1\%$ of the resources of our FPGA, making the activity undetectable. Without access to simulations of complex circuits, we instead chose several simple circuits to simulate and artificially increased the FPGA utilization in order to detect the activity. This was accomplished by adding large registers to the FPGA implementations in order for the utilization of the FPGA, and therefore the backscattered circuit activity, to be large enough to be measurable above the -140 dBm noise floor of our spectrum analyzer.

III. A NOVEL METHOD FOR COMPARING AND IDENTIFYING CIRCUITS USING REFERENCE SIMULATIONS

Three hardware implementations of circuit designs were measured in this work using the setup shown in Fig. 2: a chain of twenty cascaded inverters, a four bit counter, and an abstraction of the Advanced Encryption Standard (AES), an extremely common cypher used for cybersecurity. One difficulty with using near-field sensing of the EM backscattering side-channel is that the received power at each harmonic is not constant over time. Some harmonics have stable behavior over time with different power levels depending on the location of the 1 mm^2 area measured, while others display oscillating power measurements even at a fixed location, suggesting that such behavior is inherent to the harmonic generation and not a result of instrument noise. Fig. 4 below, in addition to showing the per-harmonic average, also shows the range of measured values received per harmonic across the chip area from the four bit counter circuit design. It is clear that the harmonic values are not consistent, with some harmonics varying up to 50 dB over the chip area. Hence, the measured minimum, maximum, and mean variation for each circuit is shown in Table 1.

It is known that higher harmonics trend toward lower received power, where both influence from noise as well as their smaller temporal resolution mean more variation

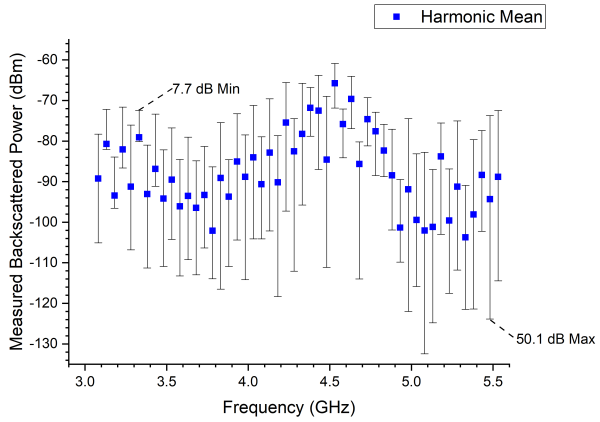


FIGURE 4. **Measured harmonic power variation using setup shown in Fig. 2 for four bit counter circuit.**

is expected. This means that the minimum variation is expected to be measured close to the fundamental frequency, and the maximum variation occurring close to the highest harmonic measured. Initially this appears to hold true for the three circuits measured, where the minimum variation occurred at harmonic 6 for all three. However, while the four bit counter and AES abstraction circuit both had their measured maximum in the last few harmonics, harmonic 49 and 48 respectively, the maximum variation for the twenty cascaded inverter circuit was measured at only harmonic 20, invalidating any expectation of a linear relationship between harmonic number and variation for a measured circuit. Furthermore, the amount of variation observed at a given harmonic was circuit dependent. For example, the variation at harmonic 29 was measured to be 15.3 dB, 42.1 dB, and 29.3 dB for the twenty cascaded inverter, four bit counter, and AES abstraction circuits, respectively. That being said, the average variation, again shown in Table 1, was relatively similar for all measured circuits, with only a 1.5 dB spread across all measured circuits. The source of these variations and their dependence on the circuit design are a result of the FPGA implementation of the measured circuits.

Many factors can change the switching characteristics of the FPGA and therefore the harmonic power received by the spectrum analyzer. These can include experimental factors such as the routing of circuit elements within the DuT or programmed timing constraints, as well as other environmental factors such as the temperature of the device, duration of operation, and other unforeseen sources of noise. Unfortunately, our simulations do not take these transient effects in the frequency domain, nor measurement variation due to spatial positions into account. The challenge then, was how to determine which set of measurement points out of thousands would be evaluated against a single simulation.

To address this, we make two reasonable assumptions. First, the main contribution to variations in our measurement is not noise. Figs. 1 and 4 show that our noise floor is 20 dB below our lowest variation and 45 dB below our lowest average measurement. Second, the circuit simulation assumes fixed environmental and temporal properties that also exist on our DuT. Depending on component utilization and other factors, circuits have different temperature profiles in different locations. Knowing this, we can assume that given an infinite number of measurements, a location matching the environmental profile of the simulation can be captured experimentally, with enough samples to also capture transient activity matching the simulation. In other words, given measurement conditions identical to those assumed by the simulation, a set of measured harmonics can be found that are identical to the spectrum of simulated harmonics. By determining how close our experimentally measured harmonics matched the simulated harmonics across all of our data we evaluate how a realistic number of measurements would compare with our lossless, noiseless, simulation. The procedure, using measurements of a perfect electric conductor (PEC) that reflects all incident energy, and a "Clean Plate", described in Section II-B is as follows:

- Take N simulation harmonics, $h_1^s, \ldots, h_n^s, \ldots, h_N^s$ and compute $N-1$ simulated harmonic ratios by performing $h_n^{s'} = h_n^s - h_{n+1}^s$.
- Measure N experimental harmonics, S times, at X x-positions, and Y y-positions, creating a 4-D matrix: $h^e_{1,1,1,1}, \ldots, h^e_{n,s,x,y}, \ldots, h^e_{N,S,X,Y}$.
- Calculate corrected "PEC" measurements by determining difference between "Clean Plate - PEC" and "Clean Plate - 50 Ohm termination" measurements, discussed in Section II-B: $\{h_1^{PEC}, \ldots, h_N^{PEC}\} = \{h_1^{pec}, \ldots, h_N^{pec}\} - \{h_1^{50\Omega}, \ldots, h_N^{50\Omega}\}$
- Augment experimental harmonics with corrected "PEC" measurements: $h^e = \{h_1^e, \ldots, h_N^e\}_{1,1,1 \to S,X,Y} - \{h_1^{PEC}, \ldots, h_N^{PEC}\}$.
- Compute mean and standard deviation, $[\mu^e, \sigma^e]$, for each "cleaned" experimental harmonic by averaging across S scans: $[\{\mu^e_{n,x,y}, .., \mu^e_{N,X,Y}\}, \{\sigma^e_{n,x,y}, .., \sigma^e_{N,X,Y}\}]$, then $X \times Y$ positions: $[\{\mu_n^e, .., \mu_N^e\}, \{\sigma_n^e, .., \sigma_N^e\}]$.
- Determine the best match for $N-1$ harmonic ratios between $h^{s'}$ and h^e using Algorithm 1.

For each harmonic, from 1 to N, we cycle through all locations and times that harmonic was measured. During this process we calculate a ratio, $h^{e'}_{n,s,x,y}$, of the current and subsequent measured harmonic. We next find the absolute difference between that measured harmonic ratio and the simulated ratio, $h_n^{s'}$. For reference, we keep track of the ratio that produced the smallest difference found for harmonic n in the "matched" ratio array, $h^{m'}$. In addition, any data points that are farther than two standard deviations from the mean are ignored in order to account for any statistical outliers. If the difference from the simulated ratio, $h_n^{s'}$, found for the current harmonic ratio, $h^{e'}_{n,s,x,y}$, is smaller than the $h_n^{s'}$, $h_n^{m'}$ difference, then the current ratio, $h^{e'}_{n,s,x,y}$, becomes the new value of $h_n^{m'}$.

This process continues until all data for the harmonic has been evaluated, and occurs for every harmonic from the first

Algorithm 1 Harmonic Matching Method

Input:

h^e of size $[N \times S \times X \times Y]$ {measured harmonics}
μ^e of size $[N]$ {mean of h^e}
σ^e of size $[N]$ {standard deviation of h^e}
$h^{s'}$ of size $[N-1]$ {simulated harmonic ratios}
$h^{m'}$ of size $[N-1]$ {empty matched array}

Procedure:

for n from 1 to $N-1$ **do** {harmonic}
  count = 0
  for x from 1 to X **do** {x position}
    for y from 1 to Y **do** {y position}
      for s from 1 to S **do** {scan}
        outlier = checkDev($h^e, n, s, x, y, \mu^e, \sigma^e$)
        $h^{e'}_{n,s,x,y} = h^e_{n,s,x,y} - h^e_{n+1,s,x,y}$
        compare_ratios = $\left|h^{s'}_n - h^{e'}_{n,s,x,y}\right|$
        curr_best = $\left|h^{s'}_n - h^{m'}_n\right|$
        if count == 0 & outlier == False **then**
          $h^{m'}_n = h^{e'}_{n,s,x,y}$
        else if compare_ratios < curr_best **then**
          if outlier == False **then**
            $h^{m'}_n = h^{e'}_{n,s,x,y}$
        end if
        count = count+1;
      end for
    end for
  end for
end for
function outlier = checkDev($h^e, n, s, x, y, \mu^e, \sigma^e$)
if $\left|h^e_{n,s,x,y} - \mu^e_n\right| > 2\sigma^e$ **then**
  outlier = true
else if $\left|h^e_{n+1,s,x,y} - \mu^e_{n+1}\right| > 2\sigma^e$ **then**
  outlier = true
else
  outlier = false
end if

Output:

$h^{m'}$ {filled matched array}

to the penultimate. It is important to note that Algorithm 1 only considers ratios of the form $h^e_{n,s,x,y} - h^e_{n+1,s,x,y}$ and not $h^e_{n,s,x,y} - h^e_{n+1,s',x',y'}$. For example, while a better match to the 5th simulated ratio, $h^{s'}_5 = h^s_5 - h^s_6$, might be found by taking the ratio of $h^e_{5,4,5,7}$ and $h^e_{6,2,8,3}$, those harmonics were measured at different positions and times so that is not an admissible ratio. In the next section, we will discuss the three circuits used in this study. Specifically, we will show the results of simulations and measurements of the activity for each circuit as well as the performance of the matching method.

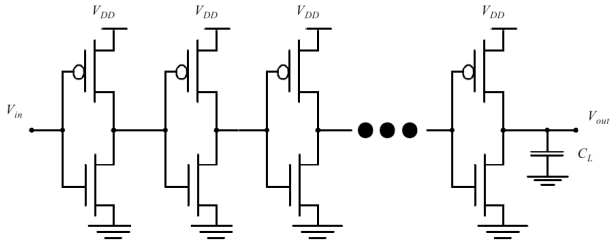


FIGURE 5. Diagram of CMOS cascaded inverters circuit.

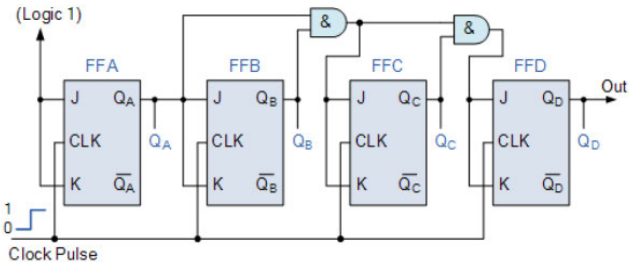


FIGURE 6. Four bit counter JK flip-flop circuit diagram.

IV. RESULTS

The first circuit that was created, shown in Fig. 5, consisted of twenty standard CMOS inverters, each containing a single pMOS and nMOS transistor, connected together in a chain. The second, more complicated, circuit that was evaluated required the creation of several basic logic gates using pMOS and nMOS transistors. AND gates, 2 and 3 gate NAND gates, and inverters were used to create four JK flip-flops that were connected to form a four bit counter. Fig. 6 contains an illustration of the simple block diagram used to create the four bit counter circuit. Lastly, in order to evaluate the performance of our method on a circuit design not only more complicated, but also more well known, we chose to implement a round of AES experimentally and in simulation. This circuit was a derivative of a single round of AES only 4 bits wide. The circuit activity starts with the output from the S-boxes, which for each bit is a different static 4 bit value. The key input is changed at half the clock speed and is stored in a flip-flop before being evaluated by a system of XOR gates which represent the ''Mix Columns'' step in AES.

A. CREATING REFERENCE SIMULATIONS

To create a true simulation of an experimental backscattering system would require a full electromagnetically accurate recreation of the DuT's circuitry, packaging, and performance characteristics within a noisy environment. This would not only be complicated and computationally challenging, but would also require exact knowledge of the internal layout and circuit interconnects of the DuT. For proof-of-concept purposes, our circuit simulations were simplistic, with ideal properties, no interconnects, and no noise sources. Despite those limitations, efforts were made to ensure that our ''Reference Simulations'' were as close as possible to the experimental measurements. The Cyclone V FPGA has a 50 MHz master clock so all simulations used a

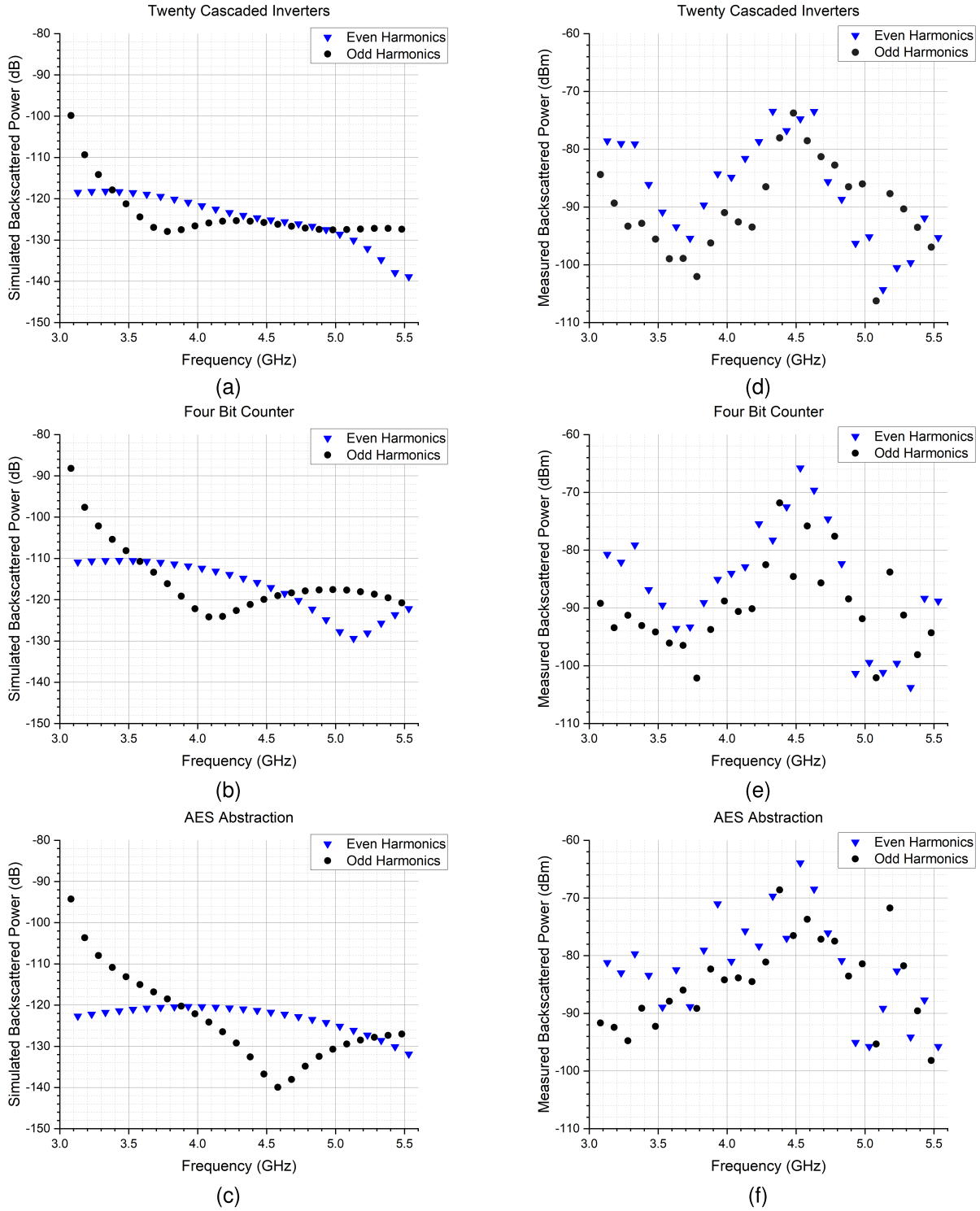


FIGURE 7. Simulated backscattered harmonics of circuit activity for (a) twenty cascaded inverters, (b) four bit counter, and (c) AES abstraction (left). Measured backscattered harmonics without clean plate augmentation of circuit activity for (d) twenty cascaded inverters, (e) four bit counter, and (f) AES abstraction (right).

clock frequency of 50 MHz. To emulate the effect of EM backscattering, we use coupled 1 mH inductors to introduce a continuous wave (CW) 3.031 GHz source to the power delivery net (VDD) of the circuits. To make the simulations as accurate as possible, the 50 MHz clock timing characteristics (a rise time of 0.469 ns and a fall time of 0.463 ns) of the FPGA design were implemented into the simulated clock [37]. Verilog circuit designs were written to ensure that the circuit designs would be implemented properly and not abstracted away, as for instance, twenty cascaded inverters is

logically identical to zero inverters. Unfortunately not every difference could be accounted for.

The Cyclone V FPGA has an SoC that uses a 28 nm low-power process node manufactured by TSMC that was originally developed by Altera and then acquired by Intel [38], [39]. The exact properties of this 28 nm node are proprietary information and as such, creating an accurate simulation that represented the behavior of the FPGA presented a challenge. The transistors used for the simulation were instead 22 nm low power models with nMOS and pMOS parameters from PTM [40]. The circuits were all powered using a constant 0.95 V voltage source and the current through VDD was measured and plotted over time. Transient analysis of the circuits was performed in Ansys EDT using a time step of 10 fs and a window of 10 μs. In MATLAB, a discrete Fourier transform (DFT) was performed on the time-series data and a plot of the frequency components was produced. These plots can be seen for each circuit in Fig. 7(a)-(c). Markers at each harmonic frequency have been added for convenience.

B. MATCHING RESULTS

In all of the simulations, shown in Fig. 7(a)-(c), the even and odd harmonics display distinct curves with the first harmonic having the strongest relative power and the rest having an average power of around -120 dB. These distinct curves are due to the lower power, but more consistent, nature of second order (even) harmonic generation compared to the higher power, but less consistent, third order (odd) harmonic generation. These results clearly illustrate that changing a circuit's design, and therefore its activity, has an effect on the simulated backscattered harmonics. Of particular interest are the similarities between the simulations of the four bit counter and AES abstraction circuits. The simulation of the AES abstraction circuit exhibits an envelope that, while being on average 10 dB down, closely matches that of the four bit counter circuit's up to 4.6 GHz. This similar, yet distinct, behavior could be a result of both circuits containing flip-flop designs, with the AES circuit using parallel D flip-flops and the four bit counter circuit using JK flip-flops in series. For comparison, the harmonic activity of all three circuits were measured using the set up shown in Fig. 2. The average of the harmonic measurements from all positions are plotted for each circuit and shown in Fig. 7(d)-(f).

With measured and simulated results gathered, we are able to evaluate the performance of our matching technique and algorithm. In addition to the three circuits described in this text, several variations of cascaded inverters including ten cascaded, five cascaded, and one single inverter were also simulated. By applying our matching method, a proper comparison between simulated and measured harmonics can be achieved and a decision on a circuit's identity can be made. While the overall number of harmonic ratios matched within 1dB is a good initial metric, we endeavor to obtain a greater understanding of the statistical properties of the match characteristics. To that end, we utilize four additional match metrics, in order to provide more confidence in a circuit identity. The first two metrics are the mean, μ, and variance, σ^2, of all 49 differences between the "matched" ratios and the simulated ratios. The third metric, maximum match error, represents the absolute value of the largest of the 49 differences. Finally, the fourth metric, skew, represents the contribution of the maximum match error compared to the sum of the error for all harmonics. A value close to 1 would indicate that the maximum value is an outlier, skewing the mean and variance to be significantly larger than they would be in the absence of that value.

TABLE 2. Matching method performance with identical circuit designs.

Circuit Design	Matches	μ [dB]	σ^2	Max [dB]	Skew
Twenty Inverters	41/49	0.99	7.06	13.2	0.271
Four Bit Counter	40/49	1.91	24.3	20.6	0.219
AES Abstraction	29/49	3.60	42.7	30.2	0.171

In Fig. 8, we are displaying three sets of harmonic ratios, all of them subtracted by the ratio of the circuit's simulation. For consistency, shapes and colors from Fig. 7 are maintained, with blue circles representing the matched harmonic ratios and the measured harmonic ratios changed to an outline. One can observe that across all circuits, the first several harmonic ratios have the worst matching performance, with other matching errors being circuit dependent, appearing sporadically throughout the range. The performance of the first few harmonics is not a huge concern to this method because, as mentioned in Section II-A, the higher harmonics offer more temporal resolution of the circuit activity.

Overall, Algorithm 1 demonstrates an impressive ability to match measured harmonics to simulated harmonics across all three circuit designs, achieving a match accuracy of < 1 dB with more than 50 % of harmonic ratios. Addressing the performance of the matching method with the AES Abstraction, the worsened match statistics are mostly a result of the extreme separation in the simulated even and odd harmonics at certain frequencies. In those situations, the harmonic ratio must exceed 20 dB at some points, which is unlikely to occur. The full statistics for the circuits tested can be seen in Table 2.

C. CIRCUIT FINGERPRINT IDENTIFICATION

So far we have shown the ability to compare and match experimentally measured harmonic activity to simulated harmonic activity of the same circuit with as high as 85% of harmonics within the match threshold. The assumption with these results is that match performance is greatest only with identical circuit designs. To this end, we test our method's matching accuracy when the simulated circuit is not the same as the experimentally measured circuit. Experimental measurements were shown in Section III to be inconsistent and because of this inconsistency, comparing an unknown circuit against other known references is much more efficient and accurate when comparing against simulations. Since we saw consistent match errors in the lower harmonics for

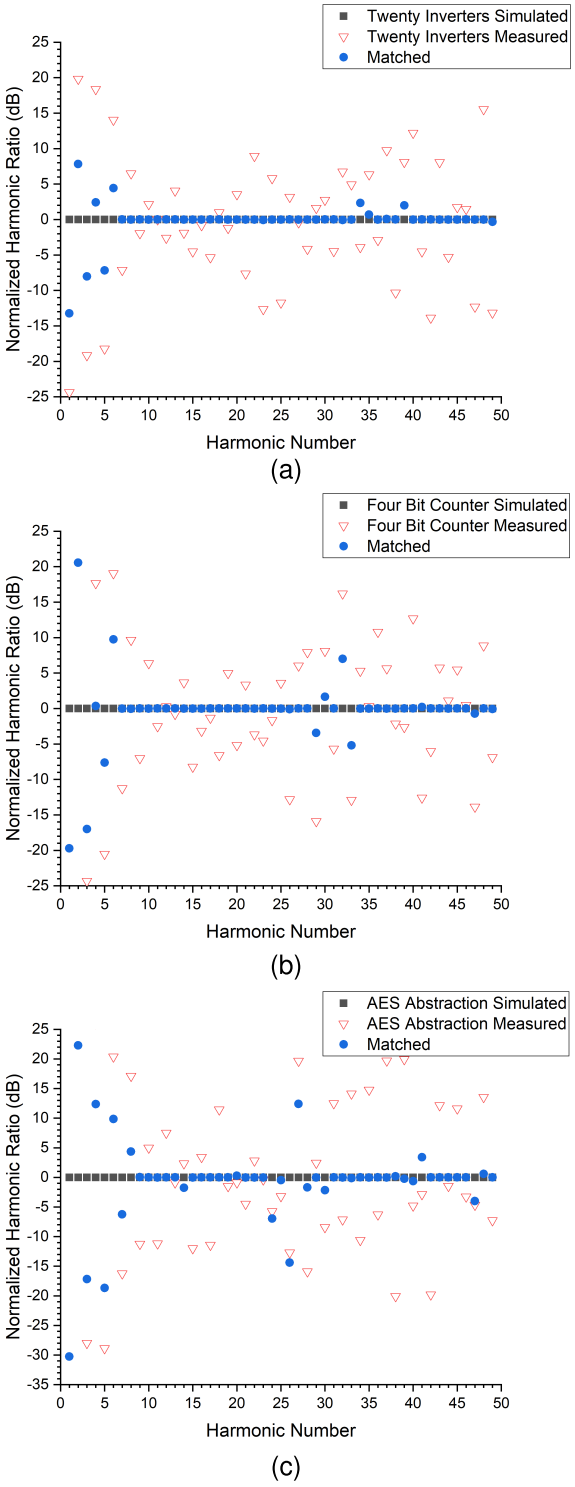


FIGURE 8. Original ($h^{e'}$) and method-adjusted measured harmonic ratios ($h^{m'}$) compared with and normalized to simulated harmonic ratios ($h^{s'}$) for (a) twenty cascaded inverters, (b) four bit counter, and (c) AES abstraction circuits.

all three circuits, and in Section II-A, described our desire for higher-order harmonics, we elect to test our method using only the last 40 harmonics. The results, including the percentage of harmonic ratios matched within the threshold,

TABLE 3. Match statistics for measured twenty cascaded inverters circuit harmonics and harmonics of dissimilar circuit simulations.

Simulated Circuit	Match %	μ [dB]	σ^2	Max [dB]	Skew
Twenty Inverters	**95.0**	**0.1**	**0.24**	**2.3**	0.410
Ten Inverters	92.5	0.4	1.59	6.9	**0.489**
Five Inverters	82.5	0.8	3.74	8.9	0.291
One Inverter	62.5	4.0	68.14	33.9	0.211
Four Bit Counter	92.5	0.3	1.28	5.7	0.473
AES Abstraction	70.0	1.7	8.31	9.1	0.137

TABLE 4. Match statistics for measured four bit counter circuit harmonics and harmonics of dissimilar circuit simulations.

Simulated Circuit	Match %	μ [dB]	σ^2	Max [dB]	Skew
Twenty Inverters	80.0	0.7	2.99	7.2	0.249
Ten Inverters	85.0	0.9	5.80	9.9	0.262
Five Inverters	85.0	0.7	2.90	8.2	0.299
One Inverter	60.0	5.0	83.76	34.8	0.172
Four Bit Counter	**90.0**	**0.4**	**2.11**	**7.0**	**0.378**
AES Abstraction	77.5	1.1	5.09	9.0	0.204

TABLE 5. Match statistics for measured AES abstraction circuit harmonics and harmonics of dissimilar circuit simulations.

Simulated Circuit	Match %	μ [dB]	σ^2	Max [dB]	Skew
Twenty Inverters	67.5	1.99	11.54	**12.3**	0.154
Ten Inverters	67.5	2.23	15.26	15.9	0.179
Five Inverters	75.0	2.02	20.55	17.5	0.216
One Inverter	60.0	4.24	50.07	23.4	0.138
Four Bit Counter	77.5	1.65	10.15	13.5	0.203
AES Abstraction	**80.0**	**1.24**	**9.94**	14.4	**0.290**

the mean error, variance, maximum error, and skew across all harmonic ratios, can be seen, along with the measured circuit and best value for each column in bold, in Tables 3-5.

We first examine the method's resistance to false positives with measured results from the twenty cascaded inverter circuit in Table 3. It is shown that by removing the first ten harmonics our match accuracy for the twenty cascaded inverter circuit is increased to 95%. In addition, while all other circuit simulations had $> 50\%$ of matches within the threshold, the twenty cascaded inverter circuit simulation had the highest overall match percentage while also maintaining the lowest variance, mean error, and max error. The closest circuit design to the twenty cascaded inverter circuit was the ten cascaded inverter circuit, with match accuracy decreasing as the number of cascaded inverters is reduced. These results suggest that to prevent false positives, a decision scheme would need to apply independent weights to each match statistic.

Table 4 shows the matching statistics for the measured four bit counter circuit, and despite the four bit counter circuit simulation matching with 10% more harmonic ratios than the twenty cascaded inverter simulation, the other match error statistics are all relatively close. The reason for this is illustrated by the final column labeled "Skew" where the maximum harmonic error has been divided by the total harmonic error. In this case, harmonic error from 38 ratios (excluding the maximum) only makes up about 60% of the total error. Using this measure is a helpful way of determining whether a match percentage is due to a majority of harmonics, or the influence of only a few.

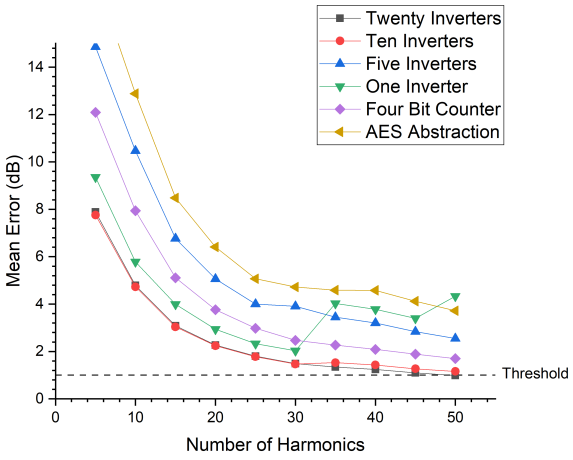


FIGURE 9. Mean threshold error for twenty cascaded inverter circuit matching results versus number of harmonics compared.

This becomes particularly relevant in the case of the AES abstraction circuit, where the least maximum error was actually found when attempting to match the twenty cascaded inverter simulation. In this case, shown in Table 5, all other match statistics are again in favor of the identical circuit designs. The maximum error measured for the AES abstraction circuit, while being 2.1 dB above that of the twenty cascaded inverter circuit, contributes almost double to the overall error. With all other statistics conclusively pointing to the simulated AES abstraction circuit, a decision on the measured circuit's identity can be made with confidence.

Fig. 9 shows that there is an inverse relationship between the number of harmonics compared and the mean error, suggesting that improving sensing techniques to capture even more harmonics would provide for even better matching performance. In addition, distinct separation between each circuit is shown, suggesting that these false positive relationships are not a property of the exact number of measurements taken, and are in fact inherent to the properties of the circuit activity itself. Additional measurements serve only to increase the resolution and allow for more accurate decisions on circuit identity. For instance, using less than 35 harmonics could produce a false positive, with the ten cascaded inverter circuit exhibiting less mean error than the twenty cascaded inverter circuit.

D. MULTI-BOARD VERIFICATION

To further show the robustness of the matching method, the final measurements performed in this study involved measuring each circuit design on multiple FPGA boards to demonstrate the method's resistance to errors from manufacturing defects. Using the exact same procedure as outlined in Section II-C, we measured four additional boards, all identical to the Cyclone V FPGA used in this study. The boards were programmed with the same circuit designs and measured with the same equipment. Using Algorithm 1, the measured results were matched to

TABLE 6. Match percentage for measured four bit counter circuit and harmonics of dissimilar circuit simulations.

Sim. Circuit	FPGA 1	FPGA 2	FPGA 3	FPGA 4	FPGA 5
Four Bit Ctr.	**84.6%**	**87.2%**	**89.7%**	**82.1%**	**89.7%**
Twenty Inv.	82.1%	82.1%	84.6%	82.1%	84.6%
Ten Inv.	79.5%	79.5%	87.2%	79.5%	85.7%
Five Inv.	79.5%	66.7%	58.9%	64.1%	74.4%
One Inv.	58.9%	53.8%	53.9%	58.9%	53.8%
AES Abstr.	79.5%	76.9%	53.9%	56.4%	56.4%

simulation, again using only the last 40 harmonics. While the results showed measurable differences between boards, there was no difference in the matching method's effectiveness and resistance to false positives. Table 6, shows the matching percentage for the measured four bit counter circuit with various simulations. The measured four bit counter circuit had the highest match percentage with the simulated four bit counter circuit on every board tested. The lowest match percentage was 82.1% for Board 4, where the simulated twenty cascaded inverter circuit had an identical match percentage as the simulated four bit counter circuit. However, by analyzing additional statistical properties, such as the fact that the twenty cascaded inverter simulation exhibited a median match error 1.5× that of the four bit counter simulation, it is clear that this result is not indicative of a false positive. Additional results comparing the match percentage for the measured twenty cascaded inverters and AES abstraction circuits show similar success in matching well to their respective simulated circuits and resisting false positives across multiple FPGAs.

V. CONCLUSION

Circuit identification has typically relied on a "Golden Chip" control that is difficult to obtain practically and increases the capture duration and amount of data required for a decision. In this work, we have shown that circuit activity from a measured circuit can be compared to simulated activity of that circuit with up to 95% accuracy and no false positives. Our circuit simulations allow our method to have the property of being "Golden Chip Free", while using near-field EM backscattering additionally allows our sensing method the benefit of non-destructive measurements. We proposed a novel calibration technique and variation compensation algorithm that allows for comparison between the unknown measured fingerprints and corresponding known simulated fingerprints suitable for a variety of applications. Future work improving the accuracy and reliability could be utilized for security applications such as counterfeit or hardware Trojan detection. In addition, demonstrations using different hardware devices and more complex simulations are needed to better determine real-world effectiveness. Finally, machine learning techniques can be applied to improve the variation compensation algorithm, or better instruments could be used to remove the need for the algorithm entirely. Further development of this sensing method will lead to greater matching accuracy and reliability enabling a broad set of applications.

ACKNOWLEDGMENT

The views and findings in this article are those of the authors and do not necessarily reflect the views of the Office of Naval Research.

REFERENCES

[1] X. Zhang, K. Xiao, and M. Tehranipoor, "Path-delay fingerprinting for identification of recovered ICs," in *Proc. IEEE Int. Symp. Defect Fault Tolerance VLSI Nanotechnol. Syst. (DFT)*, Oct. 2012, pp. 13–18.

[2] M. Ashok, M. J. Turner, R. L. Walsworth, E. V. Levine, and A. P. Chandrakasan, "Hardware trojan detection using unsupervised deep learning on quantum diamond microscope magnetic field images," *ACM J. Emerg. Technol. Comput. Syst.*, vol. 18, no. 4, pp. 1–25, Oct. 2022.

[3] M. J. Turner, N. Langellier, R. Bainbridge, D. Walters, S. Meesala, T. M. Babinec, P. Kehayias, A. Yacoby, E. Hu, M. Lončar, R. L. Walsworth, and E. V. Levine, "Magnetic field fingerprinting of integrated-circuit activity with a quantum diamond microscope," *Phys. Rev. Appl.*, vol. 14, no. 1, pp. 1–15, Jul. 2020.

[4] Y. Cheng, X. Ji, J. Zhang, W. Xu, and Y.-C. Chen, "DeMiCPU: Device fingerprinting with magnetic signals radiated by CPU," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Nov. 2019, pp. 1149–1162.

[5] F. T. Werner, J. Dinkic, D. Olcan, A. Djordjevic, M. Prvulovic, and A. Zajic, "An efficient method for localization of magnetic field sources that produce high-frequency side-channel emanations," *IEEE Trans. Electromagn. Compat.*, vol. 63, no. 6, pp. 1799–1811, Dec. 2021.

[6] 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.

[7] 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.

[8] A. Lakshminarasimhan, "Electromagnetic side-channel analysis for hardware and software watermarking," M.S. thesis, Dept. Elect. Comput. Eng., Univ. Massachusetts Amherst, Amherst, MA, USA, Feb. 2011.

[9] J. Heyszl, D. Merli, B. Heinz, F. De Santis, and G. Sigl, "Strengths and limitations of high-resolution electromagnetic field measurements for side-channel analysis," in *Proc. Int. Conf. Smart Card Res. Adv. Appl.*, in Lecture Notes in Computer Science: Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics, vol. 7771, 2013, pp. 248–262.

[10] L. N. Nguyen, C.-L. Cheng, M. Prvulovic, and A. Zajić, "Creating a backscattering side channel to enable detection of dormant hardware trojans," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 27, no. 7, pp. 1561–1574, Jul. 2019.

[11] 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.

[12] P. M. S. Sánchez, L. F. Maimó, A. H. Celdrán, and G. M. Pérez, "AuthCODE: A privacy-preserving and multi-device continuous authentication architecture based on machine and deep learning," *Comput. Secur.*, vol. 103, Apr. 2021, Art. no. 102168.

[13] F. Lorenz, L. Thamsen, A. Wilke, I. Behnke, J. Waldmuller-Littke, I. Komarov, O. Kao, and M. Paeschke, "Fingerprinting analog IoT sensors for secret-free authentication," in *Proc. 29th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Aug. 2020, pp. 1–6.

[14] H. Jafari, O. Omotere, D. Adesina, H.-H. Wu, and L. Qian, "IoT devices fingerprinting using deep learning," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Oct. 2018, pp. 901–906.

[15] S. Sangodoyin, F. T. Werner, B. B. Yilmaz, C.-L. Cheng, E. M. Ugurlu, N. Sehatbakhsh, M. Prvulovic, and A. Zajic, "Side-channel propagation measurements and modeling for hardware security in IoT devices," *IEEE Trans. Antennas Propag.*, vol. 69, no. 6, pp. 3470–3484, Jun. 2021.

[16] H. Li, A. T. Markettos, and S. Moore, "A security evaluation methodology for smart cards against electromagnetic analysis," in *Proc. 39th Annu. Int. Carnahan Conf. Secur. Technol.*, 2005, pp. 208–211.

[17] G. Baldini and G. Steri, "A survey of techniques for the identification of mobile phones using the physical fingerprints of the built-in components," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 3, pp. 1761–1789, 3rd Quart., 2017.

[18] M. Ezuma, F. Erden, C. K. Anjinappa, O. Ozdemir, and I. Guvenc, "Detection and classification of UAVs using RF fingerprints in the presence of Wi-Fi and Bluetooth interference," *IEEE Open J. Commun. Soc.*, vol. 1, pp. 60–76, 2020.

[19] S. Basak, S. Rajendran, S. Pollin, and B. Scheers, "Drone classification from RF fingerprints using deep residual nets," in *Proc. Int. Conf. Commun. Syst. Netw. (COMSNETS)*, Jan. 2021, pp. 548–555.

[20] A. Blaise, M. Bouet, V. Conan, and S. Secci, "BotFP: FingerPrints clustering for bot detection," in *Proc. IEEE/IFIP Netw. Oper. Manag. Symp., Manag. Age Softw. Artif. Intell. (NOMS)*, Apr. 2020, pp. 1–7.

[21] 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.

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

[23] 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.

[24] 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.

[25] L. N. Nguyen, B. B. Yilmaz, M. Prvulovic, and A. Zajić, "A novel golden-chip-free clustering technique using backscattering side channel for hardware trojan detection," in *Proc. IEEE Int. Symp. Hardw. Oriented Secur. Trust (HOST)*, Dec. 2020, pp. 1–12.

[26] C.-L. Cheng, L. N. Nguyen, M. Prvulovic, and A. Zajic, "Exploiting switching of transistors in digital electronics for RFID tag design," *IEEE J. Radio Freq. Identificat.*, vol. 3, no. 2, pp. 67–76, Jun. 2019.

[27] H. E. Taheri and M. Mirhassani, "A pre-activation, golden IC free, hardware trojan detection approach," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 30, no. 3, pp. 315–324, Mar. 2022.

[28] Y. Liu, K. Huang, and Y. Makris, "Hardware trojan detection through golden chip-free statistical side-channel fingerprinting," in *Proc. 51st ACM/EDAC/IEEE Design Autom. Conf. (DAC)*, Jun. 2014, pp. 1–6.

[29] H. Pearce, V. R. Surabhi, P. Krishnamurthy, J. Trujillo, R. Karri, and F. Khorrami, "Detecting hardware trojans in PCBs using side channel loopbacks," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 30, no. 7, pp. 926–937, Jul. 2022.

[30] S. Yang, T. Hoque, P. Chakraborty, and S. Bhunia, "Golden-free hardware trojan detection using self-referencing," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 30, no. 3, pp. 325–338, Mar. 2022.

[31] Y. Tang, S. Li, L. Fang, X. Hu, and J. Chen, "Golden-chip-free hardware trojan detection through quiescent thermal maps," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 27, no. 12, pp. 2872–2883, Dec. 2019.

[32] R. Yasaei, L. Chen, S.-Y. Yu, and M. A. A. Faruque, "Hardware trojan detection using graph neural networks," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, early access, May 26, 2022, doi: 10.1109/TCAD.2022.3178355.

[33] S. Faezi, R. Yasaei, A. Barua, and M. A. A. Faruque, "Brain-inspired golden chip free hardware trojan detection," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 2697–2708, 2021.

[34] J. M. Rabaey, "The CMOS inverter," in *Digital Integrated Circuits: A Design Perspective*, 1st ed. Upper Saddle River, NJ, USA: Prentice-Hall, 1999, ch. 5, pp. 144–192.

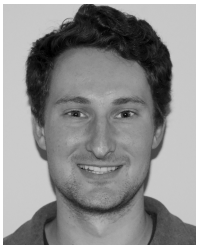
[35] L. N. Nguyen, "New side channel and techniques for hardware trojan detection," Ph.D. dissertation, Georgia Inst. Technol., Atlanta, GA, USA, 2020.

[36] C.-L. Cheng, S. Sangodoyin, L. N. Nguyen, M. Prvulovic, and A. Zajic, "Digital electronics as RFID tags: Impedance estimation and propagation characterization at 26.5 GHz and 300 GHz," *IEEE J. Radio Freq. Identificat.*, vol. 5, no. 1, pp. 29–39, Mar. 2021.

[37] Intel Corporation. (2018). *Intel Quartus Prime Standard Edition User Guide Getting Started*. [Online]. Available: https://www.intel.com/content/www/us/en/programmable/documentation/ony1529966370740.html

[38] D. Olsen, "Reducing total system cost with low-power 28 nm FPGAs," EMCC/Model. Project, Intel, Santa Clara, CA, USA, White Paper, 2015, pp. 1–6. [Online]. Available: https://www.intel.com/content/dam/www/programmable/us/en/pdfs/literature/wp/wp-01180-system-cost-low-power.pdf

[39] Altera Corporation. (2012). *Meeting the Low Power Imperative at 28 nm*. [Online]. Available: https://www.intel.com/content/dam/www/programmable/us/en/pdfs/literature/wp/wp-01158-low-power-28nm.pdf
[40] *PTM—Latest Models*. Accessed: May 13, 2021. [Online]. Available: http://ptm.asu.edu/latest.html



ANDREW S. KACMARCIK (Student Member, IEEE) received the bachelor's degree in electrical engineering from the University of Delaware, Newark, DE, USA, in 2019. He is currently pursuing the Ph.D. degree with the School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA, USA. Since 2019, he has been a Graduate Research Assistant with the Electromagnetic Measurements in Communications and Computing (EMC^2) Laboratory, Georgia Institute of Technology. His research interests include sensing methods and devices for measuring the electromagnetic side-channel of integrated circuits.

PRATEEK JUYAL (Member, IEEE) received the B.E. degree in electronics and communication engineering from Kumaun University, Nainital, India, in 2007, the M.Tech. degree in digital communication from Guru Gobind Singh Indraprastha University, Delhi, India, in 2009, and the Ph.D. degree in electrical and computer engineering from the University of Manitoba, Winnipeg, MB, Canada, in 2017. Currently, he is working as a Postdoctoral Fellow with the School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, USA. His research interests include applied electromagnetics, wireless communication, sensors, and security.

MILOS PRVULOVIC (Senior Member, IEEE) received the B.Sc. degree in electrical engineering from the University of Belgrade, in 1998, and the M.Sc. and Ph.D. degrees in computer science from the University of Illinois at Urbana–Champaign, in 2001 and 2003, respectively. In 2003, he joined the Georgia Institute of Technology, where he is currently a Professor with the School of Computer Science. His research interests include computer architecture, hardware support for software monitoring, debugging, and security. He was a recipient of the NSF CAREER Award. He is a Senior Member of ACM and the IEEE Computer Society.

ALENKA ZAJIĆ (Senior Member, IEEE) received the B.Sc. and M.Sc. degrees from the School of Electrical Engineering, University of Belgrade, in 2001 and 2003, respectively, and the Ph.D. degree in electrical and computer engineering from the Georgia Institute of Technology, in 2008. She was a Visiting Faculty Member at the School of Computer Science, Georgia Institute of Technology, a Postdoctoral Fellow at the Naval Research Laboratory, and a Design Engineer at Skyworks Solutions Inc. She is currently a Professor with the School of Electrical and Computer Engineering, Georgia Institute of Technology. Her research interests include electromagnetic, wireless communications, signal processing, and computer engineering. She was a recipient of the following awards: The Best Student Paper Award at the 13th international IEEE conference on Hardware-Oriented Security and Trust, in 2020, the IEEE Atlanta Section Outstanding Engineer Award, in 2019, the Best Poster Award at the IEEE International Conference on RFID, in 2018, the NSF CAREER Award, in 2017, the Best Paper Award at the 49th Annual IEEE/ACM International Symposium on Microarchitecture, in 2016, the Best Student Paper Award at the IEEE International Conference on Communications and Electronics, in 2014, the Neal Shepherd Memorial Best Propagation Paper Award, in 2012, the Best Paper Award at the International Conference on Telecommunications, in 2008, the Best Student Paper Award at the Wireless Communications and Networking Conference, in 2007, the IEEE Outstanding Chapter Award as a Chair of the Atlanta Chapter of the AP/MTT Societies, in 2016, the LexisNexis Dean's Excellence Award, in 2016, and the Richard M. Bass/Eta Kappa Nu Outstanding Teacher Award, in 2016. She was an Editor of IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, from 2012 to 2017, and an Executive Editor of *Transactions on Emerging Telecommunications Technologies* (Wiley), from 2011 to 2016.