Hardware Trojan Detection Through Chip-Free Electromagnetic Side-Channel Statistical Analysis

Jiaji He, *Student Member, IEEE*, Yiqiang Zhao, Xiaolong Guo, *Student Member, IEEE*, and Yier Jin, *Member, IEEE*

***Abstract*— The hardware Trojan (HT) has become a major threat for the integrated circuit (IC) industry and supply chain, and has motivated numerous developments of Trojan detection schemes. Although the side-channel method is the most promising one, nearly all of the side-channel methods require fabricated golden chips, which are very difficult to obtain in reality. In this paper, we propose a novel strategy for HT detection using electromagnetic side-channel-based spectrum modeling and analyzing. We utilize the design data at early stage of the IC lifecycle, and the generated spectrum can serve as the golden reference, and thus we do not need the fabricated golden chips anymore. Another very important feature is that our method is immune to the process variation theoretically. Experimental results on selected Advanced Encryption Standard benchmark circuits on FPGA show that our proposed method can effectively detect Trojans even with very small traces.**

***Index Terms*— Electromagnetic side channel, hardware security, hardware Trojan detection.**

I. Introduction

With an ever growing need for cost reduction, globalization of the integrated circuit (IC) industry, and supply chain, authenticity and security of the ICs are exposed to several threats. Hardware Trojans (HTs) are malicious hardware modifications to ASICs, commercial-off-the-shelf parts, microprocessors, microcontrollers, network processors, digital-signal processors, or IoTs [1]–[3]. HTs have emerged as a major security concern for ICs, which are employed in security-related situations, e.g., military, health care, aviation, communications, power management, and general critical infrastructures. HTs can be classified into analog and digital categories based on the trigger conditions [4]. Most of the Trojans can be digitally triggered and can be further divided into combinational and sequential types (see Fig. 1). Typically, sequential Trojans are usually related to main clocks or finite state machines (FSMs) of the original circuit.

To solve the problems introduced by HTs, HT detection approaches have been proposed at different stages of the whole IC lifecycle: 1) design-phase [5]–[8]; 2) test-phase; and 3) run-phase [9]–[12]. The majority of existing methods occur at test-phase, where I/O and side-channel parameters are utilized to find something abnormal. While various HT detection approaches have been explored by many researchers, statistical side-channel analyzing has been among the most heavily investigated ones. Starting with a global power consumption-based method presented in [13] and a path delay-based method introduced in [14], comparing different side-channel parameters of ICs to statistically assess whether an IC is maliciously modified by HTs has become a popular direction. Hardware security researchers have further developed similar ideas by using different kinds of side-channel measurements, including power supply transient signals [15], leakage currents [16], time-window-based supply currents [17], [18], temperature [19], light [20], electromagnetic (EM) radiation [21], [22], as well as multiparameter combinations [23], [24]. A Trojan detection method for FPGA based on a combined approach of logic-testing and side-channel analysis is proposed in [25]. In addition, there are researchers trying to strengthen the side-channel analysis through a novel statistical test generation method [26].

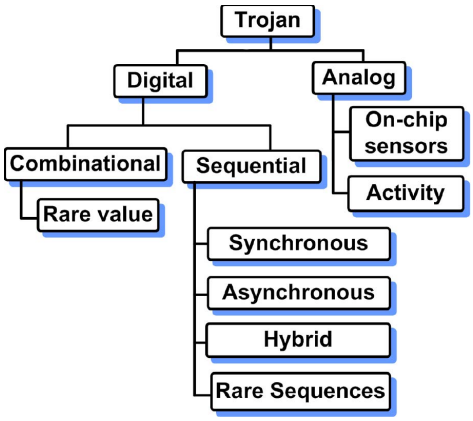

Fig. 1. HT classification based on triggering conditions [4].

However, most side-channel methods rely heavily on the existence of a trusted golden chip or other profiles alike, such as golden layout. The absence of a reliable fabricated golden chip or golden layout makes practical applications of side-channel detection approaches unfeasible. The design flow of IC begins with specifications, and then designers or vendors start coding at behavior level, using VHDL or Verilog. After codes are developed and verified through simulation, synthesis tools are utilized to convert RTL codes into gate level netlist. With outsourced third-party services, such as place & routeand

Manuscript received January 5, 2017; revised May 17, 2017; accepted June 24, 2017. Date of publication July 27, 2017; date of current version September 25, 2017. This work was supported by the National Natural Science Foundation of China under Grant 61376032. *(Corresponding author: Yier Jin.)*

J. He and Y. Zhao are with the School of Microelectronics, Tianjin University, Tianjin 300072, China (e-mail: jiaji.he@knights.ucf.edu; yq_zhao@tju.edu.cn).

X. Guo and Y. Jin are with the Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL 32611 USA (e-mail: guoxiaolong@ufl.edu; yier.jin@ece.ufl.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TVLSI.2017.2727985

fabrication, the netlist is mapped and fabricated, but the layouts and fabricated chips are untrusted. Note that there exist other untrusted sources, like third-party intellectual property cores.

In this paper, we propose a novel HT detection method through golden chip-free EM spectrum modeling and side-channel statistical analyzing. For the modeling process, an RTL design is used to generate the circuit's EM radiation. Unlike power side channel, which can be obtained from practicable softwares like PrimeTime [27], there is no such existing tool for EM side channel simulation. Especially, due to the influence of noises and variations, it will be very difficult to restore EM traces compared with actual testing results. Moreover, the traces will vary even if the position of the probe changes slightly under the same conditions. Therefore, we transform the traces from time domain to frequency domain and focus on the spectral profile of EM radiation. To the best of our knowledge, there is no such work before trying to establish EM radiation targeting FPGA implementation by taking its fan-out numbers of registers and look up tables (LUTs) into account and using the generated EM trace for HT detection. The contributions are listed as follows.

1) Simulation data from RTL are used to generate the EM spectra and the magnitude of each frequency spot. The actual executions of the circuit are taken into consideration targeting FPGA implementation. There is no need for a fabricated golden chip or a trusted layout.
2) Chirp Z-transform (CZT) and Euclidean distance algorithm are utilized to help distinguish the simulated EM spectrum from the extracted EM spectra in actual tests.
3) The proposed modeling approach is validated through FPGA experiment, and the experimental results show that Trojans can be identified with very small traces.

The rest of this paper is organized as follows. Section II gives a brief review of HTs, HT detection methods, and the comparison among different side-channel parameters. Section III gives a detailed description of the golden chip-free EM spectrum modeling methodology. In Section IV, the statistical data analyzing is introduced. In Section V, we valid the proposed model with actual testing data, and carry out a series of experiments on FPGAs. We have some discussions about the model and the experiments in this paper in Section VI. Section VII concludes this paper.

II. Background

A. Attack Model

HTs are modifications to original circuits and can generally fulfill preset functions under certain trigger conditions. Due to their stealthy characteristic, HTs are hard to get activated during functionality test and normal verification process. We assume that the design data at the RTL level are trusted, or if the design data are not trusted, the trusted circuit's functional simulation data are available, either without Trojans or with Trojans dormant. We primarily focus on digital circuits, because these circuits have certain clock signals, and the inner logic changes are key for generating the EM trace. As for the Trojans, we focus on the HT detection of sequential Trojans, because our method achieves the best results due to the Trojans' relations with the original circuit's clock and inner logic values.

B. Side-Channel HT Detection Methods

Nearly all side-channel-based HT detection methods require a trusted golden chip or a layout. Insuring a golden chip requires destructive reverse engineering of a chip [28]. Agrawal *et al.* [13] require a destructively IC fingerprint validation step to build a power fingerprint. In [14], after a path delay fingerprint has been collected, chips are examined under reverse-engineering to ensure they are the original ones. In [15], although they do not need a golden chip, a Trojan-free layout is required to serve as the trusted model. In [16], a golden model is derived from the Trojan-free layout of a chip. However, this approach is difficult to implement in practice because it is not known which chip is Trojan-free. In [17], although the TeSR method avoids the need for a golden chip, it requires a well understanding of the Trojan activation time and improvements are made in [18]. In [19], power and temperature statistics are computed using power profiles from Trojan-free layouts. In [20], a trusted layout of the chip is needed to generate emission images. The power-based side-channel analysis is cracked by a power-gated Trojan proposed in [29]. In [21] and [22], the detection of HT is successful, because they have a predefined genuine design or a golden circuit. Recently, a method without "golden model" is presented in [30], and measurements and trusted simulation models are combined together to get the trusted region. However, the requirement of precise model of the process variation makes the technique difficult. The method in [31] can be used as a golden chip free Trojan detection technique, but it has some problems when all the ICs contain the same Trojans. Meanwhile, for the postsilicon security, an on-chip classifier-based architecture for evaluating trustworthy of postdeployment is proposed in [32].

Furthermore, process variation, environment noise, and measurement noise all will cause some misalignment, and some papers have proposed strategies to tackle this problem. In [33], the intrinsic relationship between transient current I_{DDT} and quiescent current I_{DDQ} of different test vectors is exploited to eliminate the effects of the process variation. A new approach that minimizes the effect of process variation on delay via calibration using test structures is proposed in [34].

C. HTs and EM Radiation

EM radiation arises as a consequence of current flows within control, I/O, data processing, or other parts inside the chip. The currents have a correlation with logical changes performed inside the chip. Once the design is finished, the function is set, no matter what the layout or packaging of the chip will be. Each current carrying component of the circuit not only produces its radiation based on physical and electrical characteristics but also affects the radiation from other components due to coupling and circuit structure [35]. In FPGAs and CMOS devices, current only flows when there are changes in logic states, ideally. In addition, each

square-wave shaped clock edge triggers a short sequence of state changing events and corresponding currents in the data processing units. The clock will play a majority role in EM radiation, because the crystal oscillator keeps receiving and giving out currents in order to drive the whole circuit running. In addition, this has no relation with the layout or packaging of the chip. Thus, the radiation carries information about the currents and hence the events and relevant states of the interdevice. In practice, FPGAs and CMOS devices are not ideal. There exist very small leakage currents in static parts of the circuit as well, and these currents are usually relevant with the structure of these static parts. In addition, these leakage currents carry plenty useful information. Clearly, HTs are modifications to original circuits and the sequential Trojans have strong relations with clock signals, FSMs, or state nodes in the original circuits, thus will generating strong EM radiation. The HTs will influence the current flows within the ICs, and thus they will certainly affect the EM radiation of the ICs. Besides, the structural changes in the ICs, which are introduced by HTs, will cause the variations in leakage currents, which will also alter the EM radiation.

D. EM Versus Timing/Power

Agrawal *et al.* [13] utilized power signals as side-channel parameter and analyzed the effectiveness of their fingerprinting methodology for detecting Trojans using simulation methods. Following this direction, other side-channel parameters, such as temperature, timing, light, and EM profiles, are proposed. Among all these side-channel parameters, EM side channel is the most promising one. Timing-based HT detection methods usually need to use I/O ports and well-designed vectors. However, many carefully designed HTs do not influence the delay of ICs and may not be activated by traditional vectors. Power-based HT detection methods can only get a single aggregated view of the intercurrents, and power measurement usually needs a dedicated power port or a kernel power supply cable. Furthermore, when a large amount of chips are involved for trust evaluation, the noncontact EM-based approach can make the detection much faster and more efficient. Overall, EM side channel has many advantages over other side channels as follows.

1) *Noncontact Detection:* In actual EM measurement, a set of magnetic near-field probe is used to acquire the radiation. The probe is placed close right above the chip. Noncontact detection can be carried out which will be very convenient in real applications.
2) *Location Awareness:* The near-field probe can be attached to a stepper mechanism which can be controlled manually or by software via a computer. The stepper allows to step over the chip, and the accuracy of the stepper can be adjusted according to the need. One, therefore, can obtain the location-aware EM radiation.
3) *Rich in Information:* Since each active component of the circuit produces and induces various types of radiations, these radiations provide multiple views of events unfolding within the device. Different from power or timing side channels which are too vague to represent the whole characteristics of a large circuit design, the EM side channel is more powerful in detecting additional, often malicious, logic.

III. Golden-Chip Free EM Spectrum Modeling Methodology

In this section, we discuss the overall framework, algorithms, and steps included in the modeling methodology. Concerning the simulation of an IC's EM side channel, a few papers have put forward some ideas using Hamming Distance, Hamming Weight, or improved Hamming Distance model. Li *et al.* [36] introduce a Verilog&SPICE cosimulation method. A signed distance model is proposed in [37], in which they assume that charging (respectively, discharging) the capacitance involves a leakage of $+1$ (respectively, -1). From [38], different simulation methodologies in multiple levels are presented. Four models are proposed in [39], which includes: Hamming weight, Hamming distance, Hamming distance zero to one, and Hamming distance one to zero. In [40], a methodology is proposed which exports the timing back-annotated postlayout netlist and simulates it with a digital simulator.

Considering a large-scale digital IC which usually consists of tens of thousands of gates, simulation methodology like solving Maxwell equations is clearly unfeasible, since it is too complicated to deal with and it will take quite a long time. To solve this problem, we put forward a method to quickly acquire EM traces of an FPGA by calculating its signal transitions and fan-outs. While there are already some literature giving similar solutions [40], they do not give detailed steps considering the FPGA implementation. In fact, one of the contributions is an algorithm targeting FPGA implementation by taking basic elements, such as LUTs and registers into consideration. Using this methodology, the simulated traces can be quickly obtained by using ISE and ModelSim software. The simulation methodology neglects some other factors that may influence the EM radiation like the chip capitulation. The aim is modeling major part of the trace, which is caused by signal transitions. There exist some differences between the simulated trace and the real traces, and we can deal with this problem by turning traces from time domain into frequency domain and comparing particular frequency spots. Setting an appropriate threshold during traces comparison is also helpful against this mismatch, which will be specifically introduced in Section V.

The proposed model is designed for matching with actual test data. There are many other contributors for generating EM radiation, such as voltage level, but inside the circuit, it is the current that matters. The main contributors for electric current will be data transitions and driving capabilities. The initial and final states of the ith register/LUT are denoted as A_i and B_i, respectively, and t represents the moment of the transition. The transitions of all registers/LUTs in the circuit under test can be modeled as

$$D(t) = \sum_{i=1}^{n} (A_i \oplus B_i) \tag{1}$$

where $\oplus$ denotes the exclusive OR operation.

Particularly once applying this methodology using FPGAs, LUTs should be taken into consideration. The reason is that LUTs are also basic logic components like registers. Then, a tcl script, denoted as $TCLscr$, is utilized to calculate registers, LUTs, and driving capabilities. If the fan-out number of the ith register or LUT can be denoted as F_i, then the simulated EM side-channel trace can be modeled as

$$D(t) = \sum_{i=1}^{n} F_i \times (A_i \oplus B_i). \tag{2}$$

All results from (2) are added up along the time axis to get the simulated trace in time domain with every fan-out number as their weights. Also if the stimuli change, the simulated traces vary accordingly. Taking Xilinx FPGA as an example, the simulated trace in time domain is obtained through Algorithm 1.

Considering that if the original circuit is contaminated by HTs, not only states of the registers and LUTs, but also the fan-out numbers will be altered. Thus, its EM side-channel radiation will be different from the simulated one. Since the Trojan is driven by the clock signal or its division, this increases the total number of registers, hence leads to the alterations of the original trace. The above-mentioned process can be formed as

$$D(t) = \sum_{i=1}^{m} F_i \times (A_i \oplus B_i) \tag{3}$$

where $m-n$ is the number of registers introduced by the HTs.

HTs have connections with the original circuit, and they change the fan-out numbers of some registers/LUTs, which will change the value of F_i in (3). In addition, the inserted HTs can alter the internal nodes of the original circuit, which leads to the alterations of the values, including initial states, final states, or both. Specifically, it can change the values of A_i and B_i in (3).

The principal basis of the golden chip-free EM spectrum-based HT detection methodology is to find the differences between the simulated trace and the chip's actual traces from experiments. However, due to the influence of process noise, measurement noise, and environmental noise, even those chips without HTs behave slight differently considering EM side channel. Furthermore, with shrinking feature size of the ICs, process variation's influence keeps increasing on the circuit's power consumption and EM radiation in time domain. For instance, at certain points, the actual side-channel values from experiments will be higher or lower than the simulated one. Thus in time domain, if the influence introduced by HT is masked by process variation, its detection will be severely interfered. However, in frequency domain, since the EM spectrum is largely determined by the clock signal and the FSMs, both of which are insensitive to process variation, thus after Fourier transformation, the influence of process variation on EM side channel can be omitted.

Since the operating frequency of the circuit has a great impact on its EM side-channel leakage, it can reveal more information of the circuit in frequency domain. Consequently, this simulated trace is converted from time domain to frequency domain using fast Fourier transform (FFT) upon

Algorithm 1 Getting Simulated EM Side-Channel Trace

Input:
$RTL_{original}$ ▷ Original circuit description.
$Sti(t)$ ▷ Stimulation vectors at time point t.
Output: $D(t)$ ▷ The simulated EM trace at time point t.
$RTL_{synthesized} \leftarrow RTL_original$;
for Each t **do**
  $list_{registers}, list_{LUTs} \leftarrow TCLscr(RTL_{synthesized}, Sti(t))$;
  A_i, $B_i \leftarrow list_{registers}(i), list_{LUTs}(i)$;
end for
for Each A_i, B_i **do**
  $F_i \leftarrow TCLscr(RTL_{synthesized}, Sti(t))$;
end for
$D(t) \leftarrow A_i, B_i, F_i$;

which the golden chip-free EM spectrum-based HT detection methodology is built. Because of these advantages of detecting Trojans in frequency domain discussed above, the similarities and differences of the frequency spectra between the real traces from experiments and the golden trace from simulation are used to detect Trojans. Due to process variations and measurement noises, the actual EM side-channel radiation of a chip $E(t)$ is composed of E_{ori}, E_{pv}, and E_n, which are EM leakage of the original circuit, EM leakage due to process variations, and EM leakage due to measurement noises, respectively. If an HT is inserted into the original circuit, there will be an additional element E_T, which is the HT's EM side-channel information. The EM trace of a Trojan-infected chip is formulated as

$$\overrightarrow{E(t)} = \overrightarrow{E_{\text{ori}}} + \overrightarrow{E_{\text{pv}}} + \overrightarrow{E_n} + \overrightarrow{E_T}. \tag{4}$$

The impact of the noise can be eliminated by denoising, and then FFT can be applied on (4) to transform into frequency domain, as shown in the following:

$$\mathcal{F}(E(t)) = \mathcal{F}(E_{\text{ori}}) + \mathcal{F}(E_{\text{pv}}) + \mathcal{F}(E_T). \tag{5}$$

Process variation is not supposed to change frequency spot distribution of the EM side-channel spectrum, and differences caused by process variation in the magnitude of each spots are very small compared with the original value. So (5) can be further simplified as

$$\mathcal{F}(E(t)) = \mathcal{F}(E_{\text{ori}}) + \mathcal{F}(E_T). \tag{6}$$

Theoretically, if FFT is applied on the simulated trace to get $F(D(t))$, it will well correlate with $F(E_{\text{ori}})$, and they will have many identical frequency spots, as shown in

$$\mathcal{F}(E(t)) = \mathcal{F}(E_{\text{ori}}) + \mathcal{F}(E_T) \cong \mathcal{F}(D(t)) + \mathcal{F}(E_T). \tag{7}$$

The signal in time domain is $D(t)$, and its corresponding expression in frequency domain is $S(\omega)$, then according to Fourier transform, we have

$$S(\omega) = \int_{-\infty}^{+\infty} D(t) e^{-j\omega t} dt \tag{8}$$

where ω is its corresponding frequency.

The detailed composition of $\mathcal{F}(E_{\text{ori}})$ signal captured by the probe includes main clock and its harmonics, whose frequency can be denoted as $g_1, g_2, g_3 \ldots g_g$, respectively, some periodic signals generated by the circuits, whose frequency can be denoted as $f_1, f_2, f_3 \ldots f_f$, respectively, and other unintended signals, denoted as $O_1, O_2, O_3 \ldots O_o$, respectively. Assuming a sequential HT with signal transition frequency T_1 is inserted into the circuit, under the same circumstances and after FFT, the EM signal captured by the probe can be formulated as

$$\mathcal{F}(E(t)) = \sum_{i=1}^{f} A_{1i} S(j f_i) + \sum_{i=1}^{g} A_{2i} S(j g_i) + \sum_{i=1}^{o} A_{3i} S(j O_i) + A_4 S(j T_1) \quad (9)$$

where A_{1i}, A_{2i}, A_{3i}, and A_4 denote the magnitude of each frequency components, respectively.

Then, Trojan can be detected by checking the distribution of spectrum spots in the acquired EM traces. Without loss of generality, if we assume the signal transition frequency introduced by the HT is T_2, which coincides with a frequency spot of the original circuit (such as the clock signal, which is to say $T_2 = g_1$), then we can determine whether an HT has been inserted into the chip by comparing the magnitude of frequency spot g_1. If T_2 does not coincide with clock signal (which is to say $T_2 \neq g_1$), we can assume the influence of the HT as an increase of the frequency spot which coincides with one of those periodic signals. Also by analyzing the aforementioned formulae, we can judge whether an HT has been inserted into the circuit by the comparison of the magnitudes at the frequency spots. During the comparison process, FFT can be performed to transform the simulated trace to frequency domain to reveal more information concerning the frequency spots and their corresponding magnitudes.

IV. EM Side-Channel Spectral Analysis and Hardware Trojan Detection

According to the discussions in Section III, the key idea of detecting HTs is to find the differences between the simulated spectrum and actual spectra. There are three main steps to the spectral analysis and comparison process: 1) denoising the actual data; 2) zooming the spectra; and 3) comparing the two spectra.

A. Denoising

In the process of signal processing, the data measured are exposed to all kinds of noises, so denoising process is needed to optimize the data. Also variations are expected to affect spectral width of harmonics. When measuring traces through experiments, the traces are averaged using the oscilloscope to eliminate most of the random noise. After the data are stored, further denoising is performed to reduce noise and rise signal-to-noise ratio. There are two denoising methods, a traditional filtering method and a wavelet denoising method. Wavelet transform has been proved a useful tool for signal analysis and is widely used in signal processing (e.g., denoising application). The main purpose of the denoising process is to achieve both noise reduction and data feature preservation, such as transients and abrupt changes. In this context, wavelet-based methods are of particular interest. Continuous wavelet transform is denoted as

$$C_{WT}(a, \tau) = \frac{1}{\sqrt{a}} \int E(t) \cdot \psi^* \left(\frac{t - \tau}{a} \right) dt \quad (10)$$

where $E(t)$ is the signal to be analyzed (with a certain delay τ), $\psi(t)$ is the mother wavelet or the basis function, and a is a scale factor [41].

Discrete wavelet transform is a sampled version of wavelet transform. More specifically, discrete wavelet transform is computed by low-pass and high-pass filtering of the discrete time-domain signal. The signal is denoted as $E[n]$, where n is an integer. At each level, high-pass filter produces detail coefficients $d[n]$, while low-pass filter produces coarse approximations $a[n]$. Let W denote a left invertible wavelet transformation matrix of the discrete wavelet transform and taking (4) into consideration, we have

$$\begin{aligned}[a_e, d_e] &= WE = W(E_{\text{ori}} + E_{\text{pv}} + E_n + E_T) \\ &= WE_{\text{ori}} + WE_{\text{pv}} + WE_n + WE_T \end{aligned} \quad (11)$$

where $E = [E_1, E_2, \ldots E_n]$, a_e denotes the coarse approximation, and d_e is the detail coefficients.

During a short enough window period, noise signals tend to have much more changes than other signals, so detail coefficients d_e are largely composed of detail coefficients of noise in wavelet transformation domain. After removing these detail coefficients, the desired signals can be retrieved by inverse wavelet transform without much loss of other useful signals. It is a fact that resonances or coupling will cause some differences among different implementations, but they only exist in low energy domain and high frequency bands. The denoising process should also eliminate some of these useless contributions.

B. Zooming Spectra

A very high frequency resolution is needed for comparing the frequency spots and their corresponding magnitudes after FFT. Frequency estimation algorithm CZT samples along spiral arcs in the Z-plane, corresponding to straight lines in the S-plane [42]. The CZT is a signal processing technique used to analyze a portion of a spectrum at high resolution.

Specifically, CZT calculates the Z transform at a finite number of points z_k along a logarithmic spiral contour, defined as

$$z_k = A \cdot W^{-k}, \quad k = 0, 1, \ldots M - 1 \quad (12)$$

where A is the complex starting point, W is the complex ratio between points, and M is the number of points to calculate. Regions of interest are first selected out for CZT, and the resulting spectrum will have a much smaller resolution bandwidth, compared with the FFT of nontransformed data.

C. Comparing Spectra

Euclidean distance is a measure of the distance between two points in Euclidean space, and is very suitable for distinguishing experimental data from the simulated EM signal, especially

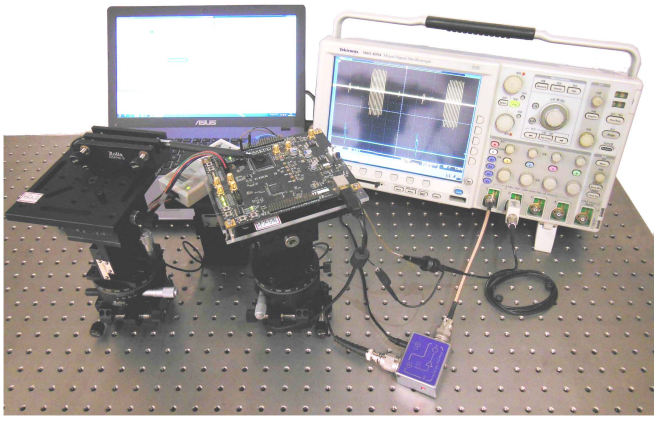

Fig. 2. Experiment setup.

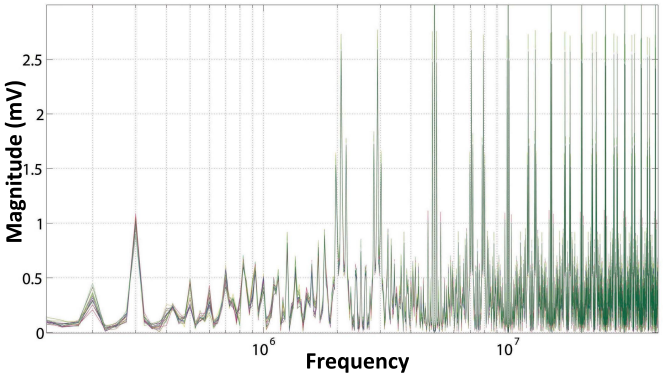

Fig. 3. Monte Carlo simulation results of S-box in frequency domain.

with the same frequency axes in both spectra. In addition, Euclidean distance is a comparatively simple and very useful method for detecting anomalies and has a high sensitivity even to small variations. Euclidean distance between points p_1 and q_1 is the length of the line segment connecting them $\overline{p_1 q_1}$. If p and q are two n-dimensional matrices, the Euclidean distance is shown in

$$d(p,q) = \sqrt{(p_1 - q_1)^2 + \cdots + (p_n - q_n)^2}. \tag{13}$$

Considering the fact that only one simulated trace from the golden chip-free model is available under one set of stimuli, there will be many actual traces of the Trojan-affected chip from experiment under the same stimuli. In order to eliminate the influence between different sets of actual data, we calculate the averaged Euclidean distance to meet the HT detection requirement.

V. Experimentation

In this section, we will validate the spectrum modeling methodology and discuss the results.

A. Experimental Setup

The experimental setup is shown in Fig. 2. FPGA platform is a SAKURA-G FPGA board [43] specifically designed for research and development on hardware security. Two Spartan-6 FPGAs are integrated on the board and serve as the controller circuit (Device: XC6SLX9-2CSG225C) and main security circuit (Device: XC6SLX75-2CSG484C), respectively. Both FPGAs are internally connected to each other. The controller FPGA provides the digital stimuli for the main FPGA and controls its operating conditions. The main FPGA is in charge of conducting out operations and will not be affected by other parts on the board. When configuring the Xilinx FPGA, PlanAhead [44] software is used to restrict the circuit into certain areas of the FPGA. So the EM radiation of the circuit will be more concentrated. A set of near field probe RF2 from LANGER [45] is utilized, and the probe is fixed on an X–Y–Z positioning system. The loop of the probe is placed right above the surface of the main FPGA to measure EM radiation. Because circuits are restricted into a certain area of the FPGA, the probe RF-R 50-1 is enough to measure the whole radiation of the circuit. Before formal tests, adjustments are made till the amplitude of the waveform in oscilloscope gets the maximum value. Then, this specific position of the probe during the whole experiments should be fixed. It is a fact that positioning variations of the probe will cause some differences in measured traces, however, in frequency domain, it will not have much influence on spectrum spots distribution but only have little influence on the energy of each spots. After acquiring EM signals by the probe, signals are amplified using a preamplifier PA303 up to 30-dB magnification. Then, the signals are captured by a Tektronix MSO4054 oscilloscope, and transferred to the control computer for further analysis.

The circuit benchmark is Advanced Encryption Standard (AES) [46], and it is an implementation of 128-bit version of the AES block cipher. However, our method is not limited to detecting HTs in cryptographic circuits. The input operands, namely, 128-bit plain text and 128-bit secret key, are provided by the controller FPGA to the main FPGA, with the on board 48-MHz oscillator. The Trojan circuits are a selection of HT benchmarks attacking an AES cryptographic circuit and these Trojans provide a wide variety of implementations. These Trojans are supplied from the Trust-HUB online repository [47], along with the original Trojan-free circuit which is the golden circuit implementation in this paper. There has been a detailed research on the benchmarks [48].

B. Process Variation Evaluation

One of the key features of the proposed method is that the EM traces are insensitive to process variations, also known as manufacturing variations. Before model verification and Trojan detection, the evaluation of process variations will be performed first. Monte Carlo simulations are used to evaluate process variation's influence on the frequency spectra. The Spartan-6 FPGA on SAKURA-G board is fabricated using a 45-nm technology, so we utilize the Monte Carlo model of a TSMC 45-nm library provided by foundry to perform the simulation.

The circuit is evaluated under the worst operating conditions defined by the library; 1000 samples are simulated and traces are transformed to frequency domain for analysis. Among all collected traces, 20 simulated Monte Carlo traces of a substitution box (S-box) in frequency domain are randomly selected and plotted in Fig. 3. Because the S-box runs at

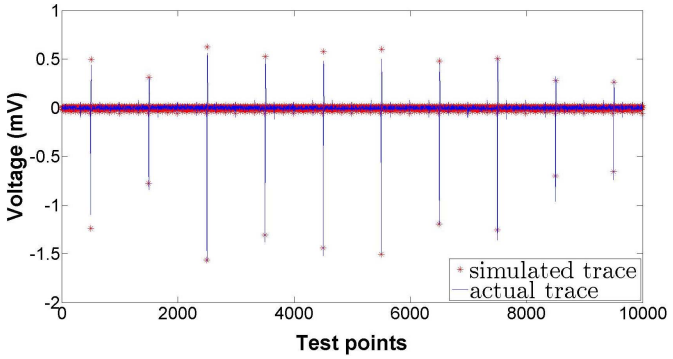

Fig. 4. S-box simulation and actual traces in time domain with two traces in one figure.

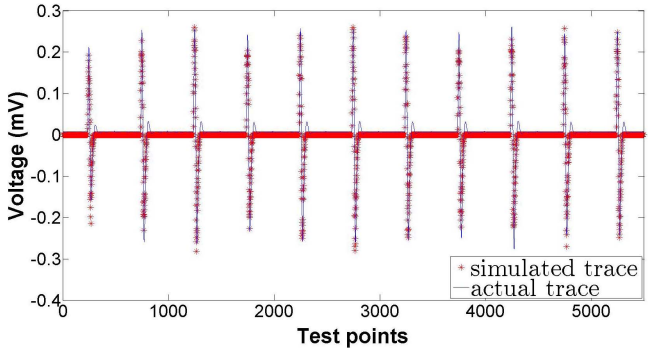

Fig. 5. AES simulation and actual traces in time domain with two traces in one figure.

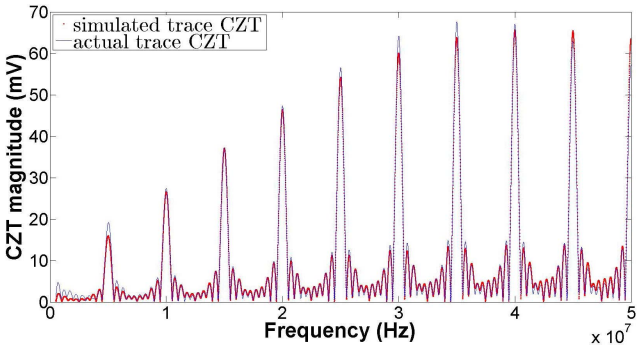

Fig. 6. AES simulation and actual traces after CZT in the frequency domain.

1-MHz frequency, so we choose 100 kHz to 10 MHz as our frequency domain, and each trace in Fig. 3 represents one Monte Carlo simulation. Histogram distribution of the frequency spectra shows that process variation does not change the frequency spots of the spectra. Analysis results of the magnitude on each spot show that process variation can only vary the magnitude within 4.68%, and more than 95% traces' differences in magnitude fall in 1.67% range. This kind of influence can be further optimized through the signal processing process, and can be omitted during our EM-based Trojan detection process.

C. Model Verification

The spectrum modeling methodology is verified by conducting out experiments on FPGA using an S-box from AES and AES itself. The S-box is a matrix used in AES cipher, and serves as an LUT in the encryption process. Because there are plenty of sequential operations, such as matrix rotating and XORing, S-box is very suitable for validation of the methodology. The S-box runs at 1-MHz frequency, and the AES runs at 5-MHz frequency. Also, the same stimuli are applied for both simulation and FPGA testing.

The simulation and actual traces of S-box in time domain are shown together in Fig. 4, and the simulated trace matches well with actual traces. The model is a success even in time domain for simple sequential circuits. The simulation and actual traces of AES in time domain are shown together in Fig. 5, and again the traces match with each other very well. Because AES runs at 5 MHz, the frequency range 500 kHz to 50 MHz is selected as the frequency of interest, and CZT is applied to transform both traces obtained from simulation and AES experiments to frequency domain. The traces in frequency domain are shown in Fig. 6. There is a very good match in low frequency band (from 500 kHz to 25 MHz), however, in high band (from 25 to 50 MHz), the model seems to have a few mismatches. We consider that it is the 48-MHz oscillator that affects the traces. In the spectrum modeling methodology, we only take the clock signal that actually drives the circuit into consideration. This is an unquestioned fact that when carrying out experiments using FPGA, the EM traces will be heavily influenced by the on board external 48-MHz crystal oscillator. Therefore, the 48-MHz on board oscillator indeed causes a few tiny mismatches. The influence introduced by the external oscillator should be the same, because the influence is the same in all experiments under the same conditions. Also, the inconsistency of the probe affects the traces measured. More specifically, amplification constant of the probe is not linear. When frequency increases, response of the probe goes higher and becomes more sensitive to the EM radiation, so there exist some mismatches between the spectra. The discordance of the probe should be taken into consideration in the future. On the whole, the simulated trace matches well with the actual traces in the frequency domain, except for a few spots.

While the presence of noise and process variation cannot be completely eliminated, we apply the Euclidean distance evaluation process to get a reference threshold, and use this threshold to show the variances of the experiment environment. If any result exceeds this threshold, then it must not be caused by environment noises (or process variations) but by HTs in the circuits.

D. Trojan Detection

To best determine how the proposed method performs in detecting Trojans, AES benchmarks are chosen from the Trust-HUB Trojan repository and there are total 21 Trojans for the AES design; 18 of these Trojans perform some sort of data-leak to compromise the integrity of the circuit. The other three Trojans (AES-T500, AES-T1800, and AES-T1900) directly attack the battery life of a power source attached to

TABLE I
HARDWARE UTILIZATION AND RESULTS OF EUCLIDEAN DISTANCE

Benchmarks	Registers	LUTs	Averaged Euclidean distance
AES	679	3137	**109.44**
AES-T100	694	3161	206.06
AES-T200	695	3180	185.07
AES-T400	1073	3409	179.93
AES-T700	669	2908	280.29
AES-T800	700	3102	171.62
AES-T900	631	2671	526.69
AES-T1000	667	2927	315.61
AES-T1100	705	3117	203.13
AES-T1200	633	2688	497.16
AES-T1600	1072	3189	288.54
AES-T1700	1018	3124	320.58

the host circuit. Besides, most of the Trojans have strong relations with clock signals of the original circuit, such as leak key covertly over many clock cycles, leak key after detecting specific sequence, or leak key after a certain number of encryptions. So we only concentrate on the 18 sequential Trojan circuits that leak the key. According to the study in [48], some of the Trojans are removed during the process of synthesizing, so we can exclude AES-T300, AES-T600, AES-T1300, AES-T1400, AES-T1500, AES-T2000, and AES-T2100. The benchmarks in the experiment will be AES-T100, AES-T200, AES-T400, AES-T700, AES-T800, AES-T900, AES-T1000, AES-T1100, AES-T1200, AES-T1600, and AES-T1700 circuits, all of which survive the synthesizing process. Also, these benchmarks all have some relations with the clock signal of the circuit. In the experiment, the Trojans are preset activated so that we can validate the proposed method better. If the Trojan remains silent, we may still be able to detect the Trojans, because their trigger parts will have influence on the EM radiation, but that requires a very high detection resolution.

The benchmarks are configured in FPGA, and the number of registers and LUTs is obtained from the implementation utilization report. For the purpose of checking the influence of HTs on circuits, the changes of total area are calculated. All data are shown in Table I. The Golden Circuit AES consumes 679 registers and 3137 LUTs. AES-T700, AES-T900, AES-T1000, and AES-T1200 consume less, and the rest seven benchmarks consume more. In fact, registers and LUTs in FPGA may not be fully utilized, and the numbers can differ according to various functions.

The real measurement traces of AES-T400 are shown in Fig. 7. All other traces are similar and we cannot find any difference between these traces. As we have mentioned in Section III, the influence of the external oscillator exists, and we cannot completely eliminate the noises and variations, so the Euclidean distances between the traces obtained from the same circuits running on the same stimuli under the same situations are calculated. This averaged Euclidean distance is used to represent the environment conditions of noise and variations. In the experiment, we calculated the reference Euclidean distance for the original AES circuit, and the result is shown in the first row in Table I. During the experimentation, any Euclidean distance that exceeds this

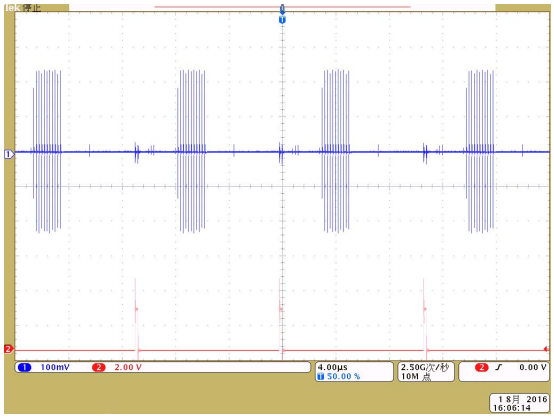

Fig. 7. Actual traces obtained from an oscilloscope for circuit AES-T400.

reference threshold indicates the existence of HTs. In order to repeat the experiments by other researchers, they should also figure out the level of the influence of noise and variations, because the environment has changed. Even if we measure the same circuits several times, the Euclidean distance calculated will be different, and this is due to the noises and variations, which actually happen in real experiments. The calculated reference Euclidean distances for 100 traces are shown in Fig. 8. The "threshold" is between 108.8 and 110.2, with a margin of 1.4, and this margin is precise enough for indicating the environment conditions and Trojan detection. With the efficient denoising and spectra zooming process, the Euclidean distance should reflect any Trojan introduced differences even with the noise and variations. So when we get the Euclidean distance between the traces obtained from the same circuits running on the same stimuli for many times, we can then give out a threshold to guide the real experiments detecting Trojans. Any Euclidean distances that are larger than the threshold Euclidean distance will consider reflecting the existence of Trojans.

Total 100 traces are collected from real experiments for each benchmark and the averaged Euclidean distances are calculated. The results are shown in the last column in Table I. The first element is the reference threshold. We can see from Table I that all the Euclidean distance results exceed the reference threshold, meaning that all Trojan circuits are successfully detected. In particular, the AES-T800 benchmark has the minimum difference compared with the reference threshold, and the margin is 62.2. The AES-T800 consumes 21 more registers and 35 fewer LUTs compared with the AES benchmark, and overall the AES-T800 consumes 130 more gates than the AES circuit. Considering that the reference threshold is between 108.8 and 110.2, the developed EM-based Trojan detection method can provide a high accuracy in detecting more challenging Trojans including those with very small fingerprints.

VI. DISCUSSION

At this stage of this paper, we introduced and experimentally validated a novel method to detect HTs. There exist many solutions that employ side-channel leakages for Trojan

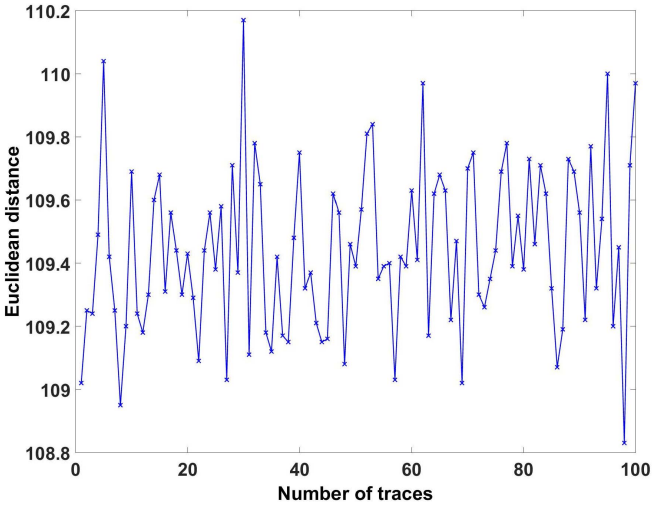

Fig. 8. Reference Euclidean distance threshold.

detection, yet most of them demand some sort of golden circuit for comparison. Eliminating the need of this requirement is thus a promising research avenue, which this paper investigates. We focus on the digital circuit carrying sequential Trojans downloaded from open resources. That is, our method achieves the best experimental results on sequential Trojans in digital circuits.

In this paper, we preset the Trojans activated to monitor the extra EM radiation caused by Trojans. However in real applications, we may need to continuously monitor the chip's EM signals, and once the Trojan gets activated, we are able to detect them. As for the Trojan activation, there are plenty studies that focus on how to activate the Trojans quickly and effectively. Salmani *et al.* [49] proposed a dummy scan flip-flop insertion procedure to decrease transition generation time for activating functional Trojans. Voyiatzis *et al.* [50] explored the applicability of the combinational testing principles for Trojan activation. An efficient test generation method was proposed in [51] considering rare events for Trojan detection. Again, how to activate the Trojan quickly and effectively is not within the scope of this paper.

VII. Conclusion

In this paper, we propose an HT detection methodology using EM side-channel-based spectrum modeling and side-channel data analyzing. We demonstrate that the simulated EM spectrum can be used as a golden reference for HT detection, and the experimental results show that the proposed method can distinguish even very small Trojans.

While our methodology is a success, some work will need to be done in the future. We should explore compensation methods at the model constructing phase for the FPGA experiments. Simultaneously, we need to seek for a better partitioning algorithm for data processing. Currently, we are able to detect the existence of HTs in the circuit-under-test. We will investigate into multiple Trojans injected design to evaluate whether our proposed method is able to distinguish different Trojans. Different Trojans should have different components in the EM radiation and the EM data should be further analyzed to derive distinct Trojan features. In addition, we plan to carry out experiments on ASIC designs in the future.

References

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

[2] Y. Jin, "Introduction to hardware security," *Electronics*, vol. 4, no. 4, pp. 763–784, 2015.

[3] J. Dofe, J. Frey, and Q. Yu, "Hardware security assurance in emerging iot applications," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, May 2016, pp. 2050–2053.

[4] R. S. Chakraborty, S. Narasimhan, and S. Bhunia, "Hardware Trojan: Threats and emerging solutions," in *Proc. IEEE Int. High Level Design Validation Test Workshop (HLDVT)*, Nov. 2009, pp. 166–171.

[5] T. F. Wu, K. Ganesan, Y. A. Hu, H. S. P. Wong, S. Wong, and S. Mitra, "Tpad: Hardware Trojan prevention and detection for trusted integrated circuits," *IEEE Trans. Comput.-Aided Design Integr.*, vol. 35, no. 4, pp. 521–534, Apr. 2016.

[6] X. Guo, R. Dutta, Y. Jin, F. Farahmandi, and P. Mishra, "Pre-silicon security verification and validation: A formal perspective," in *Proc. 52nd ACM/EDAC/IEEE Design Autom. Conf. (DAC)*, Jun. 2015, pp. 1–6.

[7] X. Guo, R. G. Dutta, P. Mishra, and Y. Jin, "Scalable SoC trust verification using integrated theorem proving and model checking," in *Proc. IEEE Symp. Hardw. Oriented Secur. Trust (HOST)*, Sep. 2016, pp. 124–129.

[8] X. Guo, R. G. Dutta, and Y. Jin, "Eliminating the hardware-software boundary: A proof-carrying approach for trust evaluation on computer systems," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 2, pp. 405–417, Feb. 2016.

[9] B. Zhou, W. Zhang, S. Thambipillai, J. T. K. Jin, V. Chaturvedi, and T. Luo, "Cost-efficient acceleration of hardware Trojan detection through fan-out cone analysis and weighted random pattern technique," *IEEE Trans. Comput.-Aided Design Integr.*, vol. 35, no. 5, pp. 792–805, May 2016.

[10] M. Lecomte, J. Fournier, and P. Maurine, "An on-chip technique to detect hardware Trojans and assist counterfeit identification," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, to be published, doi: 10.1109/TVLSI.2016.2627525.

[11] X. Zhang and M. Tehranipoor, "Ron: An on-chip ring oscillator network for hardware Trojan detection," in *Proc. Design, Autom. Test Eur.*, Mar. 2011, pp. 1–6.

[12] A. Ferraiuolo, X. Zhang, and M. Tehranipoor, "Experimental analysis of a ring oscillator network for hardware Trojan detection in a 90 nm ASIC," in *Proc. IEEE/ACM Int. Conf. Comput.-Aided Design (ICCAD)*, Nov. 2012, pp. 37–42.

[13] D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi, and B. Sunar, "Trojan detection using IC fingerprinting," in *Proc. IEEE SSP*, May 2007, pp. 296–310.

[14] Y. Jin and Y. Makris, "Hardware Trojan detection using path delay fingerprint," in *Proc. IEEE Int. Workshop Hardw.-Oriented Secur. Trust*, Jun. 2008, pp. 51–57.

[15] R. Rad, J. Plusquellic, and M. Tehranipoor, "Sensitivity analysis to hardware Trojans using power supply transient signals," in *Proc. IEEE Int. Workshop Hardw.-Oriented Secur. Trust, (HOST)*, Jun. 2008, pp. 3–7.

[16] J. Aarestad, D. Acharyya, R. Rad, and J. Plusquellic, "Detecting Trojans through leakage current analysis using multiple supply pad I_{DDQ}s," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 4, pp. 893–904, Dec. 2010.

[17] S. Narasimhan, X. Wang, D. Du, R. S. Chakraborty, and S. Bhunia, "Tesr: A robust temporal self-referencing approach for hardware Trojan detection," in *Proc. IEEE Int. Symp. Hardw.-Oriented Secur. Trust (HOST)*, Jun. 2011, pp. 71–74.

[18] T. Hoque, S. Narasimhan, X. Wang, S. Mal-Sarkar, and S. Bhunia, "Golden-free hardware Trojan detection with high sensitivity under process noise," *J. Electron. Test.*, vol. 33, no. 1, pp. 1–18, 2017.

[19] C. Bao, D. Forte, and A. Srivastava, "Temperature tracking: Toward robust run-time detection of hardware Trojans," *IEEE Trans. Comput.-Aided Design Integr.*, vol. 34, no. 10, pp. 1577–1585, Oct. 2015.

[20] F. Stellari, P. Song, A. J. Weger, J. Culp, A. Herbert, and D. Pfeiffer, "Verification of untrusted chips using trusted layout and emission measurements," in *Proc. IEEE Int. Symp. Hardw.-Oriented Secur. Trust (HOST)*, May 2014, pp. 19–24.

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

[22] 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.
[23] F. Koushanfar and A. Mirhoseini, "A unified framework for multi-modal submodular integrated circuits Trojan detection," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 1, pp. 162–174, Mar. 2011.
[24] S. Narasimhan *et al.*, "Hardware Trojan detection by multiple-parameter side-channel analysis," *IEEE Trans. Comput.*, vol. 62, no. 11, pp. 2183–2195, Nov. 2013.
[25] S. Mal-Sarkar, R. Karam, S. Narasimhan, A. Ghosh, A. Krishna, and S. Bhunia, "Design and validation for FPGa trust under hardware Trojan attacks," *IEEE Trans. Multi-Scale Comput. Syst.*, vol. 2, no. 3, pp. 186–198, Jul. 2016.
[26] Y. Huang, S. Bhunia, and P. Mishra, "Mers: Statistical test generation for side-channel analysis based Trojan detection," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Apr. 2016, pp. 130–141.
[27] *PrimeTime*. [Online]. Available: https://www.synopsys.com/implementation-and-signoff/signoff/primetime.%html
[28] C. Bao, D. Forte, and A. Srivastava, "On application of one-class SVM to reverse engineering-based hardware Trojan detection," in *Proc. 15th Int. Symp. Quality Electron. Design (ISQED)*, Mar. 2014, pp. 47–54.
[29] Y. Jin and D. Sullivan, "Real-time trust evaluation in integrated circuits," in *Proc. Design, Autom. Test Eur. Conf. Exhib. (DATE)*, 2014, pp. 1–6.
[30] Y. Liu, K. Huang, and Y. Makris, "Hardware Trojan detection through golden chip-free statistical side-channel fingerprinting," in *Proc. 51st Annu. Design Autom. Conf.*, 2014, pp. 155:1–155:6.
[31] J. Zhang, H. Yu, and Q. Xu, "Htoutlier: Hardware Trojan detection with side-channel signature outlier identification," in *Proc. IEEE Int. Symp. Hardw.-Oriented Secur. Trust*, Jun. 2012, pp. 55–58.
[32] Y. Jin, D. Maliuk, and Y. Makris, "Post-deployment trust evaluation in wireless cryptographic ICs," in *Proc. Design, Autom. Test Eur. Conf. Exhib. (DATE)*, 2012, pp. 965–970.
[33] B. Hou, C. He, L. Wang, Y. En, and S. Xie, "Hardware Trojan detection via current measurement: A method immune to process variation effects," in *Proc. Int. Conf. Rel. Maintainability Safety (ICRMS)*, Aug. 2014, pp. 1039–1042.
[34] B. Cha and S. K. Gupta, "Efficient Trojan detection via calibration of process variations," in *Proc. IEEE 21st Asian Test Symp.*, Nov. 2012, pp. 355–361.
[35] D. Agrawal, B. Archambeault, J. Rao, and P. Rohatgi, "The EM side–channel(s): Attacks and assessment methodologies," in *Proc. Cryptogr. Hardw. Embedded Syst.*, 2008, pp. 1–4.
[36] 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. (CCST)*, Oct. 2005, pp. 208–211.
[37] E. Peeters, F. X. Standaert, and J. J. Quisquater, "Power and electromagnetic analysis: Improved model, consequences and comparisons," *Integr. VLSI J.*, vol. 40, no. 1, pp. 52–60, Jan. 2007.
[38] K. Tiri and I. Verbauwhecle, "Simulation models for side-channel information leaks," in *Proc. 42nd Design Autom. Conf.*, Jun. 2005, pp. 228–233.
[39] F. Menichelli, R. Menicocci, M. Olivieri, and A. Trifiletti, "High-level side-channel attack modeling and simulation for security-critical systems on chips," *IEEE Trans. Dependable Secure Comput.*, vol. 5, no. 3, pp. 164–176, Jul. 2008.
[40] S. Bhasin, J. L. Danger, T. Graba, Y. Mathieu, D. Fujimoto, and M. Nagata, "Physical security evaluation at an early design-phase: A side-channel aware simulation methodology," in *Proc. Int. Workshop Eng. Simulations Cyber-Phys. Syst.*, Mar. 2014, pp. 13–20.
[41] O. Rioul and M. Vetterli, "Wavelets and signal processing," *IEEE Signal Process. Mag.*, vol. 8, no. 4, pp. 14–38, Oct. 1991.
[42] *CZT*, accessed on Jul. 20, 2017. [Online]. Available: http://cn.mathworks.com/help/signal/ref/czt.html
[43] *SAKURA*, accessed on Jul. 20, 2017. [Online]. Available: http://satoh.cs.uec.ac.jp/SAKURA/index.html.
[44] *PlanAhead*, accessed on Jul. 20, 2017. [Online]. Available: https://www.xilinx.com/products/design-tools/planahead.html
[45] *LANGER*, accessed on Jul. 20, 2017. [Online]. Available: https://www.langer-emv.com/en/index
[46] J. Daemen and V. Rijmen, *The Design of Rijndael: AES—The Advanced Encryption Standard*. Berlin, Germany: Springer-Verlag, 2002.
[47] *Trust-HUB*, accessed on Jul. 20, 2017. [Online]. Available: https://www.trust-hub.org/
[48] T. Reece and W. H. Robinson, "Analysis of data-leak hardware Trojans in AES cryptographic circuits," in *Proc. IEEE Int. Conf. Technol. Homeland Secur. (HST)*, Nov. 2013, pp. 467–472.
[49] H. Salmani, M. Tehranipoor, and J. Plusquellic, "A novel technique for improving hardware Trojan detection and reducing Trojan activation time," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 20, no. 1, pp. 112–125, Jan. 2012.
[50] A. G. Voyiatzis, K. G. Stefanidis, and P. Kitsos, "Efficient triggering of Trojan hardware logic," in *Proc. IEEE 19th Int. Symp. Design Diagnostics Electron. Circuits Syst. (DDECS)*, Sep. 2016, pp. 1–6.
[51] S.-J. Wang, J.-Y. Wei, S.-H. Huang, and K. S.-M. Li, "Test generation for combinational hardware Trojans," in *Proc. IEEE Asian Hardw.-Oriented Secur. Trust (AsianHOST)*, Sep. 2016, pp. 1–6.

Jiaji He (S'17) received the B.S. degree in electronic science and technology and the M.S. degree in microelectronics from Tianjin University, Tianjin, China, in 2013 and 2015, respectively, where he is currently pursuing the Ph.D. degree at the School of Microelectronics.

He is currently a Visiting Scholar with the University of Central Florida, Orlando, FL, USA, under the guidance of Y. Jin, from 2016 to 2017. His current research interests include digital circuit design and hardware security.

Yiqiang Zhao received the B.S. degree in semiconductor physics and device, the M.S. degree in microelectronics, and the Ph.D. degree in microelectronics and solid-state electronics from Tianjin University, Tianjin, China, in 1988, 1991, and 2006, respectively.

In 1991, he joined the Jinhang Technical Physics Institute, Tianjin, where he was responsible for analog and mixed signal circuit design. Since 2001, he has been with the School of Electronic Information Engineering and the School of Microelectronics, Tianjin University, where he is currently a Professor. His research interests include mixed-signal integrated circuits, security chips, and hardware security.

Xiaolong Guo (S'14) received the double B.S. degree from the Beijing University of Posts and Telecoms (BUPT), Beijing, China, and the University of London, London, U.K., in 2010, and the M.S. degree from BUPT in 2013. He is currently pursuing the Ph.D. degree in electrical and computer engineering at the University of Florida, Gainesville, FL, USA.

His current research interests include design of scalable verification methods for hardware IP protection, trusted SoC verification, cyber security, formal methods, program synthesis, and secure language design.

Yier Jin (M'13) received the B.S. and M.S. degrees in electrical engineering from Zhejiang University, Hangzhou, China, in 2005 and 2007, respectively, and the Ph.D. degree in electrical engineering from Yale University, New Haven, CT, USA, in 2012.

He is currently an Associate Professor with the ECE Department, University of Florida, Gainesville, FL, USA. His research focuses on the areas of trusted embedded systems, trusted hardware intellectual property (IP) cores, and hardware–software coprotection on computer systems. He proposed various approaches in the area of hardware security, including the hardware Trojan detection methodology relying on local side-channel information, the postdeployment hardware trust assessment framework, and the proof-carrying hardware IP protection scheme. He is also interested in the security analysis on Internet of Things (IoT) and wearable devices with particular emphasis on information integrity and privacy protection in the IoT era.

Dr. Jin received the DoE Early CAREER Award in 2016 and the Best Paper Award of DAC'15, ASP-DAC'16, and HOST'17.