Fundamental Limit and Performance Tradeoffs in DCR-based Power Side-Channel Attack Trojan Detection Circuits

***Abstract*—The globalization of the semiconductor supply chain has created ample opportunities for adversaries to embed hardware trojans in various production stages. Many researchers have identified a malicious probing resistor as a low-cost and effective Trojan to launch power side-channel attacks. This paper presents the first analyses on the fundamental limit and performance tradeoffs of generic and energy-efficient DC resistance (DCR) based power side-channel trojan detection circuits. This paper found the minimal detectable resistance to be a function of the circuit's thermal noise and the desired statistical significance of the detection. With this knowledge, designers can predict the detection performance from specifications before any transistor design. This paper illustrated that environmental factors, such as temperature, supply impedance, and supply voltage, appear as common-mode signals. Hence, they do not affect detection performance in the first order. This paper also suggested that data-driven averaging could be used to reduce thermal noise, which offers a valuable tradeoff between detection time and accuracy. Simulations results from IC blocks designed in a 65-nm CMOS process confirmed the above analyses.**

***Index Terms*—Hardware Trojan, side-channel attack, Trojan detection, impedance measurement, binary classification, integrated circuit noise**

I. Introduction

A side-channel attack(SCA) is an eminent threat to secure hardware devices. Secure devices are responsible for handling sensitive data. This data can appear on side channel information (power signature, EM radiation, timing, etc) of a device. An adversary can collect and process this information to extract the secret key. If the key gets exposed, the device is no longer secure. The attacker can use this key to draw out sensitive [1] information. This information can be in the form of electromagnetic (EM) [2] emission, power [3] consumption, timing variation, acoustic noise, etc. This work provides a direct relation between minimum detectable sense resistor which can be used to predict circuit parameters. There are various tradeoffs related to the use of a topology, performance parameters and detection efficiency. This work explains different scenarios related to various conditions including external factors, environmental factors and fundamental limits imposed on detection of a sense resistor. The way of thoroughly characterizing this approach provides a deep insight into design of detection circuits, which can be used to improve or further develop even more robust detection techniques.

II. Background

Power side-channel attack (P-SCA) uses plain text sent to the encryption device. A sense resistor can be inserted into the power supply of the device. The power consumption is measured on the oscilloscope after the insertion of the resistor. The information on this side channel can be collected and analyzed by techniques like simple power analysis [4], differential power analysis [3] or correlational power analysis [5].

The design requirements for a modern encryption device are stiff due to the requirements posed by hardware security. Countermeasure techniques helps in increasing immunity. Recent works have shown various algorithms [6] and hardware used techniques [7]–[9] to mitigate these concerns, leading to higher immunity towards side-channel attacks.The adversary can still draw out sensitive information given enough time and resources.

The attacker can overcome immunity for given system with enough time and resources. The approach to proactively detect an attack is popular in recent works [10]. Detection circuits using machine learning (ML) show successful implementation in this direction [11], [12] . The technique use ML training models to monitor nodes in a power delivery network (PDN). These models are trained offline and can detect an attack in real time. This type of approach can detect and mitigate attacks as compared to increasing the immunity of a device. The ML based techniques come with power and area overheads. The requirement to train ML models and have a number of sensors for monitoring increases complexity of the approach.

Detection of impedance on power delivery network has also been used in RO based detection approach [13]. This technique uses an on chip ring oscillator to monitor change in the impedance of node in a PDN. RO based method monitors any change in the impedance of a ball gird array (BGA) for insertion of SCR. Any change in the BGA impedance results in change of number of transitions and phase. The differential change of a compromised node and normal operation can be used as a metric to detect the attack. If the attack is performed on the whole PCB impedance instead of a C4 bump in a BGA, the whole grid would adjust according to the supply. In this case a differential signal would not be available to detect an attack. A monitoring of total PCB impedance using a SC circuit [14] provides detection in this case. This techniques uses a SC circuit to monitor the total power supply impedance. The insertion of a sense resistor is detected by the SC circuit. The above mentioned techniques using RO based and SC circuit further simply the detection approach as they don't come at the cost of large area and power overhead.

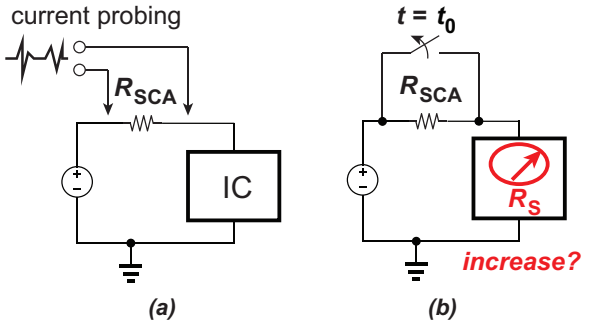

Fig. 1. (a) Threat Model (b) Assumption and Detection Method.

TABLE I
P-SCA DETECTION METHOD COMPARISON

	TCAS-I [12]	ICCAD [13]	This Work [14]
Threat Model	Current probing via an external R_{SCA}		
Detection Method	PDN sensing	ΔV sensing	R_S sensing
Sensor circuit	ADC	Ring OSC	Switch-cap
Sensor number	Multiple	Multiple	Single
Classification	Data Intensive	Simple	Simple
R_{SCA}@ BGA	YES	YES	YES
R_{SCA}@ PCB	YES	NO	YES

These techniques don't require ML training models or any data storage from tests.

A. Threat Model

Fig. 1 (a) shows the common threat model of a power side-channel attack assumed by prior work [11]–[15] and this paper. The adversary inserts an attack resistor R_{SCA} anywhere along power trace coming into the victim IC. [13] further assumed that the R_{SCA} replaced one of the BGA (bird grid array) package balls through package hacking, but [11], [12], [14], [15] did not make such a specific assumption.

Another assumption of prior work [11]–[15] and this paper is that R_{SCA} is inserted at a specific time during the victim's operation, as shown in Fig. 1 (b). The precise time of R_{SCA} insertion (t_0) is unknown to the victim. Hence, the goal for the power side-channel attack (P-SCA) detection system is to detect such an insertion accurately with minimal delay.

B. Detection Method

Fig. 1 (b) also shows the proposed detection method. Any *unexpected* supply resistance (R_S) *increase* is used to detect the intrusion of an R_{SCA}. Our previous work [14] has shown its advantages over prior art in power, area, computation requirements, and detection coverage. These advantages are summarized in Table I.

III. PROPOSED CIRCUITS AND SYSTEMS

A. System Architecture

Fig. 2 shows the system architecture of the on-chip R_{SCA} detection circuits.

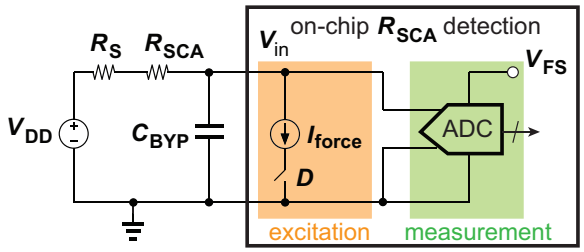

Fig. 2. System Architecture for on-chip R_{SCA} detection. (V_{FS}: ADC's full-scale reference, C_{BYP}: total bypass capacitance, R_S: total parasitic resistance, including R_{BAT}, R_{PCB}, and $R_{IC,package}$)

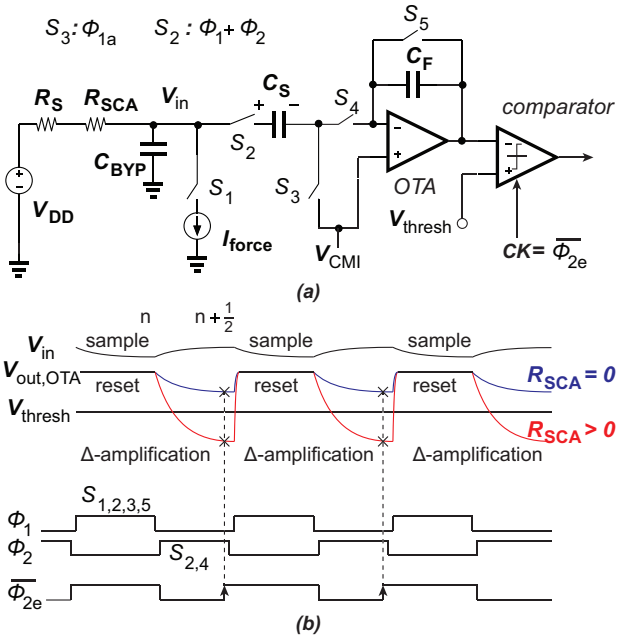

Fig. 3. (a) Switched-capacitor Δ-THA circuit implementation (b) Timing and Waveforms: Non-overlapping clocks (ϕ_1, ϕ_2) and early clocking (ϕ_{2e}) for the comparator

It consists of two sub-systems – excitation and measurement. The excitation system is an on-chip current source (I_{force}). The measurement system is a single-bit or multi-bit analog-to-digital converter (ADC). To measure the DC resistance (DCR) of the supply line, I_{force} is periodically pulled on V_{in} with duty cycle D. As a result, V_{in} would experience a commensurate, periodic IR-drop (ΔV). With ΔV measured by the ADC, the DCR can be calculated as:

$$DCR = \frac{\Delta V}{I_{force}} \tag{1}$$

If the DCR deviates from the expected R_S, an R_{SCA} intrusion is detected.

B. Circuit Implementation

Fig. 3 (a) shows a switched-capacitor circuit implementation [14] of the excitation and measurement systems. The switched-capacitor circuits was used as the measurement system because it was simpler than a full-blown ADC. Switch S_1 and current

sink I_{force} constitute the excitation system. The measurement system includes a switched-capacitor, $\Delta-$modulated Track-and-Hold Amplifier ($\Delta-$THA), a pre-determined threshold voltage (V_{thresh}), and a comparator. The measurement circuits operate as follows:

During ϕ_1, switch $S_{1,2,3,5}$ are closed. V_{in} settles to to its first final value: $V_{in,1}$ due to IR-drop:

$$V_{in,1} = V_{DD} - I_{force}(R_S + R_{SCA}) \tag{2}$$

At the end of ϕ_1, $V_{in,1}$ is sampled across C_S. Bottom plate sampling [16] is used to open S_3 in advance with ϕ_{1a}. For ease of analysis, assume $V_{CMI} = 0$. The charge stored on C_S and C_F are:

$$Q_S : -V_{in,1}C_S \qquad Q_F : 0 \tag{3}$$

During ϕ_2, switches $S_{1,3,5}$ open and switches $S_{2,4}$ close. V_{in} recovers to its second final value $V_{in,2}$.

$$V_{in,2} = V_{DD} \tag{4}$$

Since S_2 is also closed during ϕ_2, C_S amplifies the difference between $V_{in,1}$ and $V_{in,2}$ via charge redistribution and amplification through C_F and OTA. This operation is similar to the delta compression often used in neural recording [17], [18]. If we adopt the discrete-time index of $[n]$ and $[n+\frac{1}{2}]$ to mark the voltages at the end of ϕ_1 and ϕ_2, $V_{in}[n] = V_{in,1}$ and $V_{in}[n+\frac{1}{2}] = V_{in,2}$. At the discrete time $[n+\frac{1}{2}]$, the charge stored on C_S and C_F are:

$$Q_S : -V_{in}[n+\frac{1}{2}]C_S \qquad Q_F : -V_{out}[n+\frac{1}{2}]C_F \tag{5}$$

Equate the sum of Eq. 3 and Eq. 5:

$$V_{out}[n+\frac{1}{2}] = \frac{C_S}{C_F}(V_{in}[n] - V_{in}[n+\frac{1}{2}]) \tag{6}$$

$$= G(V_{in,1} - V_{in,2})$$

$$= -GI_{force}(R_S + R_{SCA}) \tag{7}$$

$G = C_S/C_F$ is the close-loop gain. Fig. 3 (b) shows the timing diagram and waveforms of the implemented circuits. Depending on whether R_{SCA} is present, $V_{out}[n+\frac{1}{2}]$ would settle to a higher or lower value. Just before the end of ϕ_2, $V_{out}[n+\frac{1}{2}]$ is compared against V_{thresh} to detect if R_{SCA} is present. An early rising edge ($\overline{\phi_{2e}}$) derived from the logic inverse of ϕ_2 can be used as the comparator clock.

IV. Fundamental Limit

A. Minimal Detectable R_{SCA}

Though some prior work [11]–[13], [15] has qualitatively described the relationship between the value of R_{SCA} and the performance of detection, we here derive a quantitative expression of the minimum detectable R_{SCA} ($R_{SCA,min}$) using our proposed circuits.

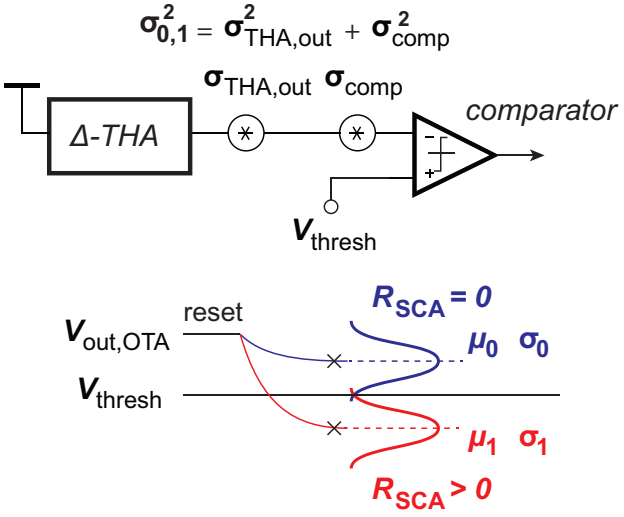

Fig. 4. The uncertainty model for the detection circuit

There are multiple sources that will introduce uncertainty to the final detection. First, $V_{out}[n+\frac{1}{2}]$ in both secure (blue curve in Fig. 4) and compromised (red curve in Fig. 4) scenarios present voltage uncertainty. Secondly, the comparator presents trip point uncertainty due to its input-referred thermal noise, flicker noise, and offset. Lastly, the on-chip current sink I_{force} may have errors due to V_{DS} difference and process mismatch. Thus, to simply analysis, we will make the following assumptions.

Assumption 4.1 (Perfect I_{force}): I_{force} is error free.

In practice, this assumption can be well approximated by trimming. Process variations and mismatch can be trimmed away during production tests so that I_{force} is within one LSB of the desired target. The post-trim I_{force} value can also be measured by the Automatic Test Equipment (ATE) and stored on-chip for easy access.

Assumption 4.2 (Perfect $1/f$ and offset cancellation): The comparator has perfect offset and flicker noise cancellation.

In practice, autozeroing, correlated double sampling, and chopper stabilization can be applied to eliminate those imperfections in CMOS comparators [19].

Under these assumptions, Fig. 4 models the sources of uncertainty in the proposed detection circuit. The uncertainty in $V_{out}[n+\frac{1}{2}]$, i.e., $u(V_{out}[n+\frac{1}{2}])$, is assumed to be dominated by the track-and-hold (THA) circuit output noise. [1] It is modeled as a normal random variable with standard deviation of $\sigma_{THA,out}$. The uncertainty in the comparator trip point is assumed to be dominated by the comparator's input-referred noise. It is modeled as another random variable with standard deviation σ_{comp}. Since these two noise sources come from different circuits, we assume $\sigma_{THA,out}$ and σ_{comp} are uncorrelated. Hence, the combined *uncertainty* for detection can be modeled as a result of the total *noise* σ_{out}:

[1] Pedestal error, sampling jitter, and aperture delay can all affect $u(V_{out}[n+\frac{1}{2}])$. However, assuming that V_{out} is fully settled and comparator is clocked slightly earlier (at ϕ_{2e}) than ϕ_2 switches open, their impact can be minimized.

$$\sigma_{out}^2 = \sigma_{THA,out}^2 + \sigma_{comp}^2 \tag{8}$$

The average values for $V_{out}[n+\frac{1}{2}]$ under a secure and compromised configuration can be expressed as μ_0 and μ_1. If V_{reset} is the output voltage of the THA circuit during reset, $\mu_{0,1}$ can be found from Eq. 7 as:

$$\mu_0 = V_{reset} - GI_{force}R_s \tag{9}$$
$$\mu_1 = V_{reset} - GI_{force}(R_s + R_{SCA}) \tag{10}$$

The standard deviation of for $V_{out}[n+\frac{1}{2}]$ under the secure and compromised configuration can be expressed as σ_0 and σ_1. From Eq.8, $\sigma_0 \approx \sigma_1 = \sigma_{out}$ as long as R_{SCA} does not increase $\sigma_{THA,out}$ significantly. This is often a reasonable assumption, because R_{SCA} is of small value, which contribute little to thermal noise. In addition, a well-designed track-and-hold circuit's output noise is often dominated by the OTA, not the input branch resistance [20].

Next, we formulate the problem of power side-channel attack detection as **hypothesis testing**: We seek to reject the null hypothesis (H_0) with significance level of α.

- H_0: System is secure. ($R_{SCA} = 0$).
- H_1: System is compromised. ($R_{SCA} > 0$).

The significance level α is the probability of making a Type-I error, i.e., rejecting H_0 when it is true. Correspondingly, the probability of making a Type-II error, which is accepting H_0 when H_1 is true, can be expressed as β.

Without loss of generality, assume that Type-I (false positive) and Type-II (false negative) cost equally to the detection system. (More on the rationale in Section IV-B.) Since $\sigma_0 = \sigma_1 = \sigma_{out}$, the detection threshold voltage V_{thresh} should be set as:

$$V_{thresh} = \frac{\mu_0 + \mu_1}{2} \tag{11}$$

Fig. 5 is the basis for the derivation of $R_{SCA,min}$. The distance between μ_0 and μ_1 compared to σ determines the achievable α and β value. When R_{SCA} used by the adversary is small, the difference in mean value ($|\mu_1 - \mu_0|$) is too small compared to their standard deviations (σ_1, σ_0). Hence, there may be not V_{thresh} that can satisfy a given P-SCA detection significance (α, β) requirements. On the other hand, if the R_{SCA} used by the adversary is big, $|\mu_1 - \mu_0|$ is large enough compared to σ_1, σ_0 so that a range of V_{thresh} can simultaneously satisfy α, β requirements.

As a result, the minimal detectable R_{SCA} resistance is a function of σ, $|\mu_1 - \mu_0|$, and α, β. The desired significance level will decide how many σ's μ_1 and μ_0 need to be separated. We express this minimum separation requirement as a function: $f(\alpha, \beta)$. For example, if assume $\alpha = 0.05$ (95% confidence in rejecting H_0), and $u(V_{out}[n + 1/2])$ follows Gaussian distribution with $\sigma_0 = \sigma_1 = \sigma$:

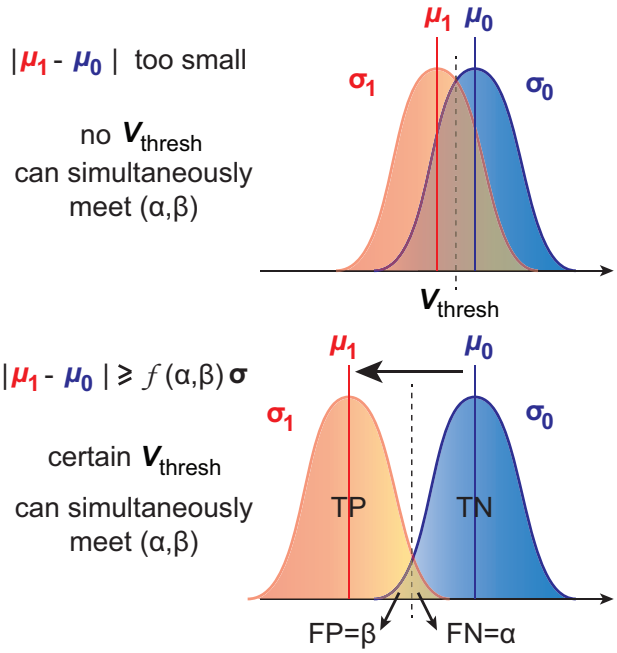

Fig. 5. Derivation for the minimal detectable resistance: $R_{SCA,min}$

$$\alpha = 1 - \phi(\frac{|V_{thresh} - \mu_1|}{\sigma}) \leq 0.05 \tag{12}$$
$$\Leftrightarrow |V_{thresh} - \mu_1| \geq 1.645\sigma \tag{13}$$

$\Phi(z)$ is the cumulative distribution function of a standard Gaussian distribution: with zero mean and standard deviation of one: $\phi(z) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{z} e^{-x^2/2}\, dx$. The value 1.645 can be found numerically or by reading a Z table [21]. Similarly,

$$\beta = 1 - \phi(\frac{\mu_0 - V_{thresh}|}{\sigma}) \leq 0.05 \tag{14}$$
$$\Leftrightarrow |\mu_0 - V_{thresh}| \geq 1.645\sigma \tag{15}$$
$$\therefore |\mu_0 - \mu_1| \geq 2 \times 1.645\sigma = 3.29\sigma \tag{16}$$

Thus, $f(\alpha, \beta) = 3.29\sigma$ when $\alpha = \beta = 0.05$. For higher confidence level (e.g., 99%), $f(\alpha, \beta)$ will increase and can be calculated accordingly. For general hypothesis testing significance requirements, Eq. 16 can be written as:

$$|\mu_0 - \mu_1| \geq f(\alpha, \beta)\sigma_{out} \tag{17}$$

Plug in Eq. 9 and 10 into Eq. 17:

$$GI_{force}R_{SCA} \geq f(\alpha, \beta)\sigma_{out} \tag{18}$$
$$R_{SCA} \geq \frac{f(\alpha, \beta)\sigma_{out}}{G \cdot I_{force}} \tag{19}$$

Therefore, the minimal detectable R_{SCA} for a given detection accuracy (i.e., significance α, β requirements for a binary hypothesis testing) is found as:

TABLE II
DEFINITION OF THE CONFUSION MATRIX ELEMENTS

	Detected as PSCA (pos)	Detected as Secure (neg)
True PSCA	True Positive (TP)	False Negative (FN)
True Secure	False Positive (FP)	True Negative (TN)

$$R_{SCA,min} = \frac{f(\alpha,\beta)}{GI_{force}} \cdot \sigma_{out} \tag{20}$$

Where σ_{out} models the combined *uncertainty* in the form of total *noise* at the output of the THA circuit. To gain more insight to the design, we can refer σ_{out} to the input of the THA:

$$R_{SCA,min} = \frac{f(\alpha,\beta)}{I_{force}} \cdot \sigma_{in} \tag{21}$$

Where σ_{in} models the input-referred *uncertainty* in the form of input-referred noise. Plug in Eq. 8:

$$\sigma_{in} = \sqrt{\sigma_{THA,in}^2 + \frac{\sigma_{comp}^2}{G^2}} \tag{22}$$

A few observations can be made from Eq. 21:

1) Input-referred thermal noise of the IC (σ_{in}) prevents the detection of an arbitrarily small R_{SCA}. THA and comparator contribute to σ_{in}, as shown in Eq. 22.
2) High significance levels $f(\alpha,\beta)$ also raises $R_{SCA,min}$.
3) A 2x increase in I_{force} cuts $R_{SCA,min}$ by half. But it also doubles the excitation system's power consumption. Similarly, more power can be spent in the measurement system to reduce σ_{in} and $R_{SCA,min}$. Thus, there may be an optimal approach to achieve $R_{SCA,min}$ with minimum total power.
4) The absence of V_{DD} and R_S in Eq. 21 suggests that the proposed detection theme is immune to environmental factor variations.

Some of these observations are further explored in Section V.

B. Evaluation Metrics

The proposed P-SCA detection system essentially performs a binary classification, i.e. where the IC at any given time t is secure ("0") or under attack ("1"). Hence, commonly used binary classification evaluation metrics can be applied to measure the "accuracy" of the proposed system and circuits. Detection time and circuit overheads are also used to evaluate the proposed detection circuits.

1) Accuracy: Like many other binary classification tasks, the PSCA detection circuit "effectiveness" can be evaluated using the confusing matrix $M = \begin{pmatrix} TP & FN \\ FP & TN \end{pmatrix}$ [22]. The definition of each element of M in the PSCA detection context is defined in Table II.

Additional performance measures, such as accuracy, precision, recall (sensitivity), specificity, F-1 score, and Matthews Correlation Coefficients (MCC) [23], can also be used to evaluate specific strength and effectiveness of the PSCA detection circuit. A summary of these metrics is provided in Table III.

TABLE III
ADDITIONAL EVALUATION METRICS AND INTERPRETATION

	Formula	Interpretation
Accuracy	$\frac{TP+TN}{TP+TN+FP+FN}$	overall effectiveness
Precision	$TP/(TP+NP)$	% SCA detected
Recall (sensitivity)	$TP/(TP+FN)$	(pos) correct ratio
Specificity	$TN/(FP+TN)$	(neg) correct ratio
F-1 score	$\frac{2TP}{2TP+FP+FN}$	0:wrong, 1:perfect
MCC	see [23]	-1:wrong, 1: perfect

For different applications, different measures in Table III are preferred. For example, in text classification, precision/recall pair are used extensively, even though these two measures are invariant to TN [22]. MCC is also considered superior to F-1 score in un-balanced datasets. The discussion on which set of measures are the most appropriate for cyber situation classification is beyond the scope of this paper and worthy of future research. The assumption of equal cost of Type-I and Type-II error is assumed without loss of generality.

2) Detection Time: The detection time (t_{DET}) can be defined as:

$$t_{DET} = t_1 - t_0 \tag{23}$$

t_0 indicates the time when a P-SCA is launched by the adversary. t_1 is the time that the proposed circuit rejects the "secure" hypothesis H_0 with a specific power of significance (α,β). Small t_{DET} is essential because the side-channel power analyses can be completed rather quickly [15]. If t_{DET} is longer than the completion time of a P-SCA, the benefit of having a detection is nullified as the adversary has already retreated the sensitive information.

3) Power, Performance, Area Overhead: Like other fully integrated power side-channel attack detection circuits [12], [13], the power, performance, and area (PPA) overhead of the proposed P-SCA detection circuits is of interest. Smaller PPA overhead while achieving the same security assurance is highly desirable due to cost structure (in die area, design effort, and test cost) for ICs [24].

There are two ways to compare PPA overhead among different P-SCA detection circuits: the absolute overhead and the relative overhead. Both are valid approaches, and different work's PPA overhead can be compared across different technology nodes as long as the baseline system-on-chip (SoC) PPA is the same or comparable, and that CMOS feature-size advantages are fully accounted for. One caveat is that some approaches [11], [12] require off-chip training. Though not directly part of the PPA overhead, the machine learning model's training time, epoch, and data size present additional costs and overhead for SoC end-users.

V. Performance Tradeoffs

A. Environmental Factors

An ideal P-SCA detection circuit should have minimal variation with environmental factors. Observation 4) in in Section IV-A suggested that our proposed method can be immune to V_{DD}, R_S, and temperature changes. The key to understanding this feature is that these variations appear as common-mode signals. Therefore, their variations do not affect the differential-mode signals which the detection is based upon. Hence, the proposed scheme is first-order immune to supply voltage V_{DD}, supply impedance R_S, and ambient temperature variations.

Specifically, V_{DD} appears as a common-mode signal during $\Delta-$THA operation. Eq. 7 ensures that V_{DD} is cancelled as $V_{in,2}$ is subtracted from $V_{in,1}$. Similarly, R_S also appears a common-mode signal as evident in Eq. 9 and 10. The $GI_{force}R_S$ term is cancelled as μ_1 is subtracted from μ_0 in deciding the fundamental limit. Lastly, ambient temperature may or may not affect the detection performance. Their impact will be analyzed and simulated in Section VI-B2.

B. Speed vs. Accuracy Tradeoff

1) THA Speed Accuracy Tradeoff: The selection of clock speed f_{clk} is a tradeoff between speed and accuracy within the generic ADC or the proposed track-and-hold (THA) circuit in the architecture shown in Fig. 2. The minimal time for to obtain a single measurement on $V_{out}[n+\frac{1}{2}]$ is a clock period T, as shown in the timing diagram of Fig. 3 (b). A faster clock can reduce T, but it can also increase the settling error at the sampling instants $(n, n+\frac{1}{2})$. This clocking speed vs. accuracy tradeoff in the measurement circuits are consistent with speed/accuracy tradeoff in THA [20], [25] or residue amplifier [26], [27] designs for high-performance ADCs. State-of-the-art approaches to address the tradeoff include digital calibration for incomplete setting [28], adjustable bandwidth OTA [25], integrator-based OTA [29], or dynamic amplifier OTAs [30]. These methods come with their advantages and limitations.

Specifically in the proposed P-SCA detection architecture (Fig. 2), T is limited by the RC product of off-chip bypass capacitance (C_{BYP}) and the source impedance (R_S). It is common for IC to apply C_{BYP} at power input to filter out supply noise. Assume a low footprint $C_{BYP} = 0.47\mu F, R_S = 1\Omega$, the RC time constant $\tau \approx 0.5\mu s$. Assume 1% settling accuracy requirement, the maximum clock speed would be:

$$f_{CLK} = \frac{1}{T} \leq \frac{1}{2 \times 5\tau} = 200kHz \tag{24}$$

2) System Speed Accuracy Tradeoff: The proposed architecture in Fig. 2 can also adopt averaging across multiple clock period for additional speed and accuracy tradeoff. By averaging the detection decisions over N cycles through majority voting, zero tolerance [12], or data-driven noise reduction [31], the input-referred noise σ_{in} can be further reduced. With a smaller σ_{in}, the achievable $R_{SCA,min}$ can be reduced (Eq. 21. In addition, a smaller σ_{in} also reduce Type I and Type II error rate (α, β) when detecting the same R_{SCA} used by the adversary. This can be understood by inspecting the left-hand side of Eq. 12. A reduction in σ_{in} reduces σ_{out}, which increases the ϕ value and reduces α.

This improvement in α, β would also translate to a more ideal confusion matrix M, as well as higher F-1 and MCC scores. However, these improvements come at the price of NT instead of T in the detection time, as well as addition circuits to implement the N-cycle averaging techniques.

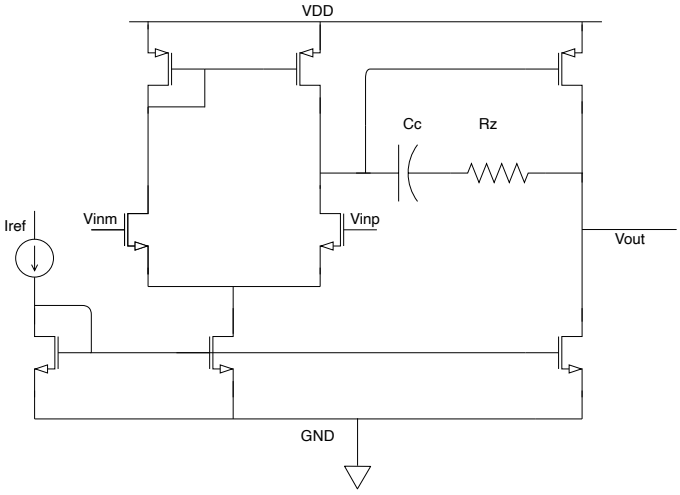

Fig. 6. An NMOS-input two-stage opamp used as the THA OTA

VI. Simulations Results

A. On Fundamental Limit

In order to verify the fundamental limit on $R_{SCA,min}$ derived in Eq. 21, we will adopt the following methodology:

- Start with initial objective specs (IOS): $R_{SCA,min} = 1\Omega$ and desired significance of 95% ($\alpha = \beta = 0.05$)
- Design circuits with noise performance to achieve (1).
- Simulate the designed circuits with and without power side-channel attacks (P-SCA). During P-SCA, $R_{SCA} = 1\Omega$
- Verify that $R_{SCA} = 1\Omega$ can indeed be detected with significance α, β. Compare the actual detection performance with predicted performance through the confusion matrix.

1) Initial Objective Spec (IOS): We start with an IOS on $R_{SCA,min}$ as 1Ω and desired $\alpha = \beta = 0.05$. For low power operation, we choose $I_{force} = 100\mu A$. Hence, the expected $|\mu_0 - \mu_1| = 100\mu A \times R_{SCA,min} = 100\mu V$. Given $f(\alpha, \beta) = 3.29$, the circuit's σ_{in} should be less than $30.4\mu V_{rms}$.

2) Circuit Design with Targeted Noise Performance: The circuits in Fig. 3 was designed and simulated in a TSMC 65-nm CMOS process. An NMOS-input two-stage operational amplifier with lead compensation [16] was used as the OTA, as shown in Fig. 6. A close-loop gain of $G = \frac{C_S}{C_F} = 30$ is chosen with $C_F = 1pF$. Metal-insulator-metal (MIM) capacitor were used to implement both C_S and C_F. Common centroid layout technique was used to achieve good matching to reduce G variation with device mismatch.

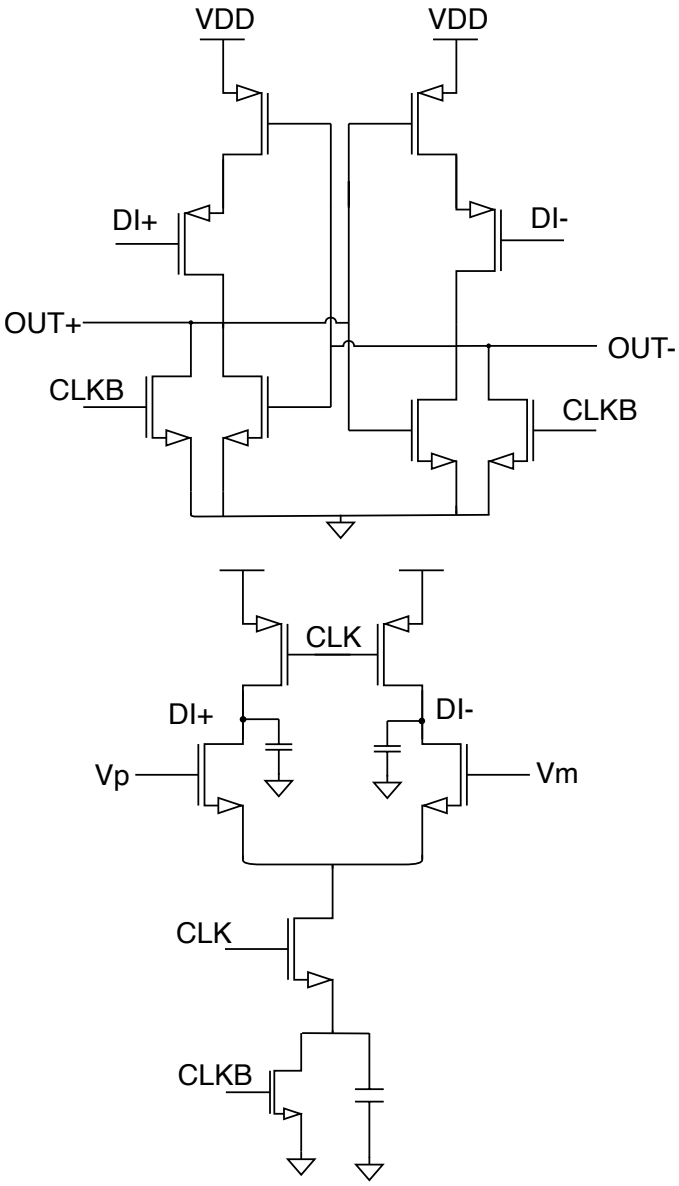

Fig. 7. Comparator used for measurement

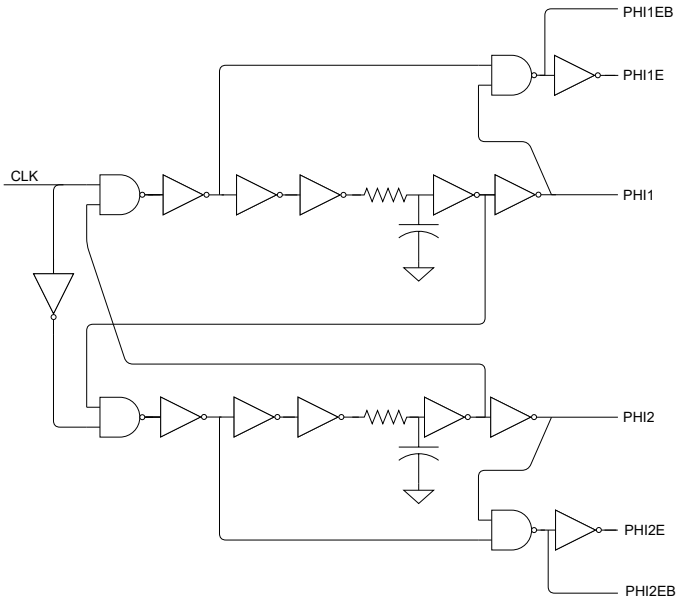

Fig. 8. Clock generation circuit

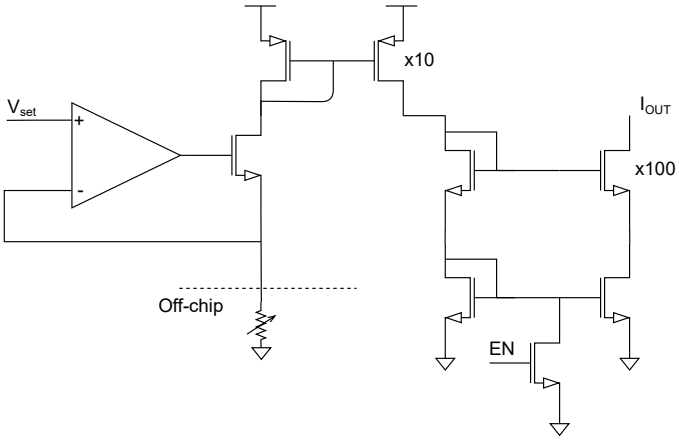

Fig. 9. Current array

A dynamic comparator [32] was used to create a single-bit decision of "safe" (0) versus "compromised." (1). The schematic of the comparator is shown in Fig. 7. The choice is mainly driven by the need to reduce comparator's input-referred thermal noise. As explained in [32], the source degeneration capacitor effectively pushes the input pair of the comparator into subthreshold region toward the end of pre-amp phase in order to increase g_m/I_D and reduce σ_{comp}.

Fig. 8 shows the non-overlapping clock generator used to create ϕ_1, ϕ_2, ϕ_{1e}, and ϕ_{2e}. ϕ_{1e} for bottom plat sampling is generated by the AND function of ϕ_1 and an earlier version of ϕ_1. The RC low pass filter within the delay chain ensures that the non-overlapping time is sufficient across PVT variations. Fig. 9 shows the cascoded current mirror that implements I_{force}. I_{out} generates the current sink to V_{in}. I_{in} is a reference input current generated from a V-to-I converter. (not shown in Fig. 9.) But adjusting the external voltage and resistor, I_{in} can be tuned so that I_{out} (a.k.a. I_{force}) can be trimmed to the desired accuracy. Duty cycling of the current mirror is controlled through the EN MOSFET.

The OTA and the comparator are built with core devices, and they operate under $V_{DIG} = 1.0V$. Switch S_1 and S_2 are built with I/O PMOS devices for safe, direction connection to $V_{DD} = 2V$. C_{BYP} is chosen to be $0.47\mu F$ to balance between supply noise rejection performance and the speed of the proposed circuit's operation. R_S is modeled to be $250m\Omega$: $100m\Omega$ from the IC bondwire resistance and $150m\Omega$ to emulate AA battery impedance.

The output noise of the track-and-hold amplifier (THA) circuit ($\sigma_{THA,out}$) is simulated with Cadence transient noise simulations. Fig. 10 shows the $V_{out}[n + \frac{1}{2}]$ waveform over time under a safe (green curve: $R_{SCA} = 0$) and compromised

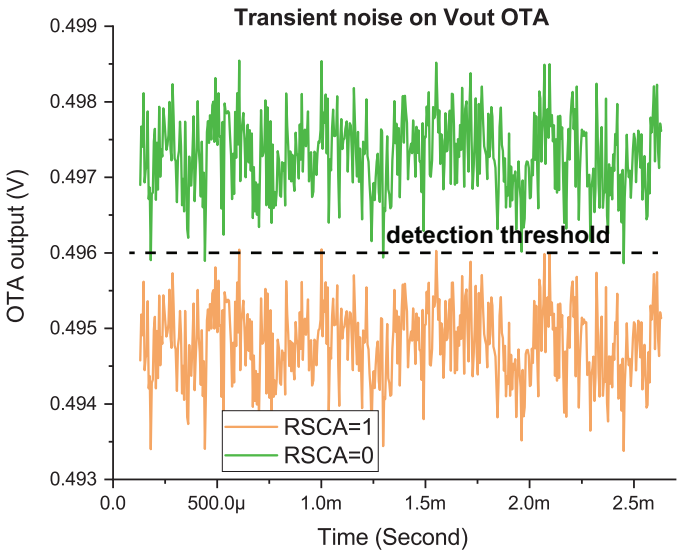

Fig. 10. Transient noise simulation: sampled $V_{out,OTA}$ over time

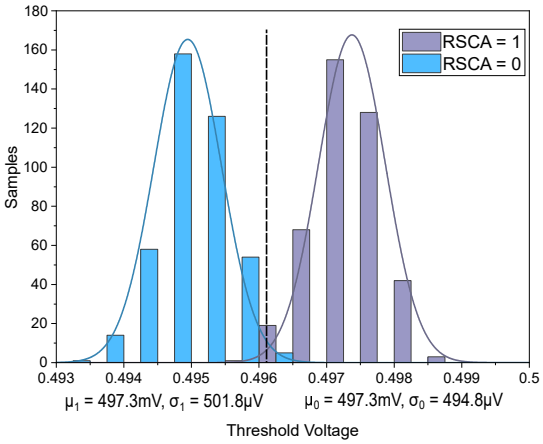

Fig. 11. Noise distribution at the output of OTA

(orange curve: $R_{SCA} = 1\Omega$) configuration. First, the output voltage of the THA amplifier (V_{out}) is ideally sampled through Cadence calculator function just before the comparator is activated (at the rising edge of ϕ_{2e}) to capture the noise present on V_{out} at the time of comparison (discrete time $n+\frac{1}{2}$, $n = 1, 2, \cdots$). Next, the ideally sampled time series of $V_{out}[n+\frac{1}{2}]$ is plotted in OriginLab over time as Fig. 10. As seen in Fig. 10, the two scenarios are separated enough for a detection threshold voltage (V_{thresh}) to be set in the middle.

The mean (μ_0, μ_1) and standard deviations (σ_0, σ_1) of $V_{out}[n+\frac{1}{2}]$ can be measured by plotting the histogram for the time series data in Fig. 10 into Fig. 11. A total of 1196 data points on $V_{out}[n+\frac{1}{2}]$ for both secure (R_{SCA} = 0) and compromised (R_{SCA} = 1) scenario were plotted in Fig. 11. μ_0 corresponds to the mean value on $V_{out}[n+\frac{1}{2}]$ when the IC is secure, and it is found to be 497.3 mV. μ_1 corresponds to the mean value on $V_{out}[n+\frac{1}{2}]$ when the IC is under an P-SCA attach with $R_{SCA} = 1\Omega$. μ_1 is found to be 494.9 mV. The standard deviations σ_0 and σ_1 are found to be identical

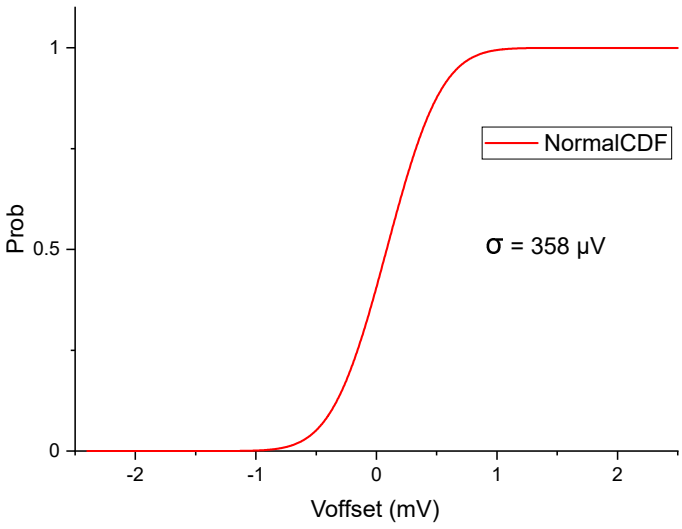

Fig. 12. Input referred noise of the comparator standalone

up to $0.1\mu V$:

$$\sigma_1 = \sigma_2 = \sigma_{THA,out} = 501.2\mu V \tag{25}$$

Next, the input-referred noise of the dynamic comparator is simulated following the time-domain technique described in [33]. Transient noise simulation is run on the comparator over a large number of comparisons with various input differential voltages. The number of samples used for this simulation was 5990. The normal CDF fit for varying offset voltage provides the input referred noise of the comparator: $\sigma_{comp} = 358\mu V$.

Following Eq. 8, the total noise can be calculated as:

$$\sigma_{out} = \sqrt{\sigma_{THA,out}^2 + \sigma_{comp}^2} = 616\mu V \tag{26}$$

Notice Eq. 8 approximate well under assumption 4.1 and 4.2. However, the dynamic comparator and the OTA in Fig. 7 and Fig. 6 do not have auto-zero or offset cancellation techniques applied. Hence, assumption 4.2 may not be valid, and that Eq. 8 may have underestimated the real σ_{out} in this design.

A more accurate measurement for σ_{out} will be to simulate σ_{out} directly. According to the uncertainty model in Fig. 4, σ_{out} can be measured directly if we keep R_{SCA} constant (in either secure or compromised configuration) and sweep V_{thresh} as we run N periods of continuous comparisons with transient noise turned on. Fig. 13 shows the output probably of "1" over the range of V_{thresh} near μ_0. A Gaussian Cumulative Distribution Function (CDF) curve fitting measures $\sigma_{out} = 989\mu V$. This is indeed higher than the ideal σ_{out} calculated from Eq. 26, since all the nonidealities, such as current source noise, THA offset, comparator offset and $1/f$ noise are all included. Refering σ_{out} noise to the input, we measure $\sigma_{in} = \sigma_{out}/G = 989\mu V/30 = 33\mu V$, which meets the IOS.

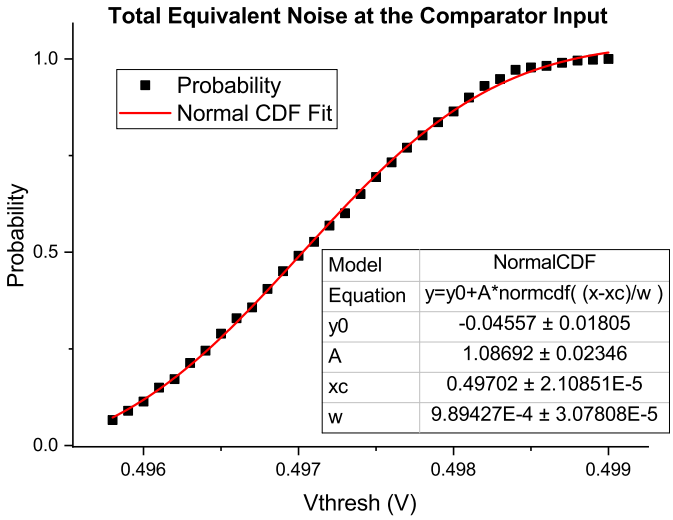

Fig. 13. Direct Simulation for σ_{out} in secure $R_{SCA} = 0$ configuration.

3) Verify Predictions and Compare Performance: Given the initial objective specs on circuit noise, I_{force}, and significance level α, β, $R_{SCA,min}$ can be predicted without running any system level simulations. According to the Eq. 21:

$$R_{SCA,min} = \frac{f(\alpha,\beta)\sigma_{in}}{I_{force}} = \frac{3.29 \times 33\mu V}{100\mu A} = 1.086\Omega \quad (27)$$

Next, we will run system level simulations with and without power side-channel attacks (P-SCA) and see if the system can detect both cases correctly. When a P-SCA is launched, we choose to use $R_{SCA} = 1\Omega$, which is just at the $R_{SCA,min}$ predicted. When simulating a secure configuration, R_{SCA} is set to 0Ω. R_{SCA} is inserted along the V_{DD} supply trace at time $t_0 = 126\mu s$ and remain for the rest of the transient simulation. The detection circuit is continuously clocked at $f_{CLK} = 200kHz$ with no data averaging used at the comparator output.

In the truly secure test case, $R_{SCA} = 0$. But due to circuit noise, there could be certain periods where the comparator would report "1". This simulates the false positive (FP) rate in the proposed detection scheme. Most other periods the comparator would output "0". This simulates the true negative (TN) rates. Likewise, in the truly compromised test case, $R_{SCA} = 1\Omega$. Due to circuit noise, certain periods would report "0". That emulates the false negative (FN) rate. In most of the periods, the comparator would output "1", which simulates the true negative (TP) rates.

The simulations run for 1196 clock periods. The total count of positive (POS) and negative (NEG) detection results were collected to calculate the simulated confusion matrix. This confusion matrix can be compared against the predicted ones. Predicted confusion matrix is based on predicted TP, TN, FP, FN. Given the IOS, they can be predicted as follows:

TABLE IV
COMPARISON OF PREDICTED AND SIMULATED P-SCA DETECTION PERFORMANCE

$R_{SCA} = 1\Omega$	Predicted	Simulated
True Positive	88.9 %	95.0 %
False Negative	11.1 %	5.0 %
False Positive	11.1 %	6.6 %
True Negative	88.9 %	93.4 %

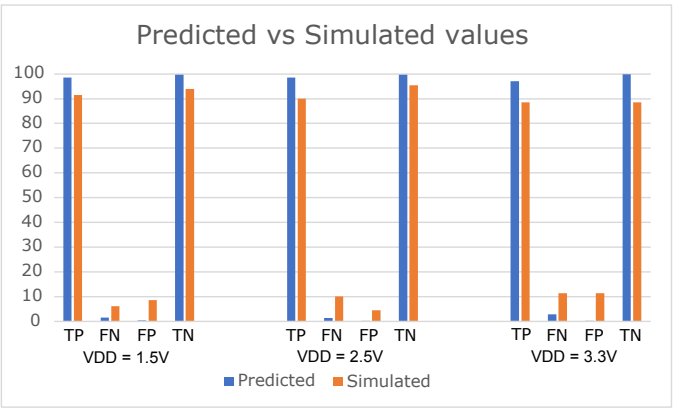

Fig. 14. Variation of simulated vs predicted results.

$$TP = \phi(\frac{V_{thresh} - \mu_1}{\sigma_{out}}) \quad (28)$$

$$FN = 1 - TP \quad (29)$$

$$TN = 1 - FP \quad (30)$$

$$FP = \phi(\frac{V_{thresh} - \mu_0}{\sigma_{out}}) \quad (31)$$

Table IV shows the simulated confusion matrix with respect to the predicted one. First, the probe resistance $R_{SCA} = 1\Omega$ is indeed detected with close to 95% significance for both Type I and Type II error. This confirms the correctness of the fundamental limit described in Section IV-A, Eq. 21. Secondly, the simulated confusion matrix match well with the predicted values, which confirms that designers can indeed predict the detection performance of the resulting system *before* transistor design, as long as the circuit's noise performance can meet the initial objective specs.

B. On Performance Tradeoffs

1) Supply voltage variation: Supply voltage V_{DD} variation should not affect the detection performance in the first order, as analyzed in section V-A. The system level simulations are run at $V_{DD} = 1.5V, 2, 5V, 3.3V$. The resulting simulated confusion matrix are listed below. The simulations are based on 596 consecutive clock cycle of transient noise simulations.

Fig 14 shows the simulated confusion matrix parameters versus their predicted values under all three V_{DD} test cases. The variation is minimal and matches with the predicted result

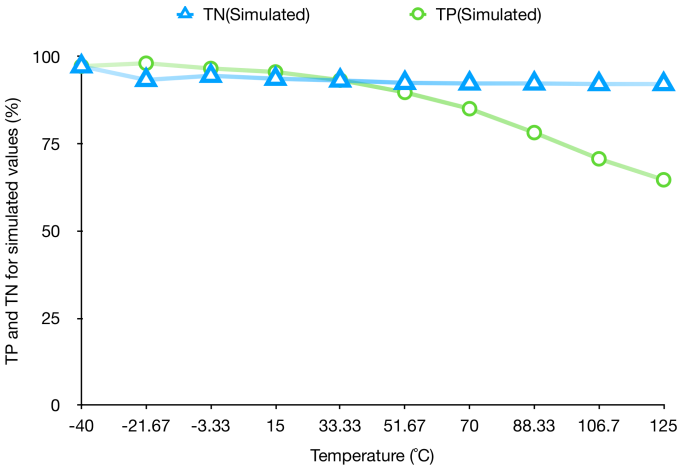

Fig. 15. Accuracy of TP and TN for temperature variations

$$M_{V_{DD}=1.5} = \begin{bmatrix} 91.45\% & 8.5\% \\ 6.1\% & 93.9\% \end{bmatrix}$$

$$M_{V_{DD}=2.5} = \begin{bmatrix} 89.9\% & 10.1\% \\ 4.5\% & 95.5\% \end{bmatrix}$$

$$M_{V_{DD}=3.3} = \begin{bmatrix} 88.6\% & 11.4\% \\ 4.5\% & 95.5\% \end{bmatrix}$$

2) Temperature Variation: The circuit performance has dependence on temperature variations. The circuit on package have a slight different behaviors with change in temperature as compared to the one from source resistance and R_{SCA}. The source resistance can depend on the PCB fabrication as it can vary based on the battery. On the other hand R_{SCA} is the resistance introduced by an attacker and depends on the quality of resistor. For this analysis it is safe to assume that the adversary would use a high quality resistor with minimal variation with temperature to reduce footprint on insertion in the circuit.

System-level simulations were run to find out the confusion matrix for different operating temperatures. Fig. 15 shows the TP and TN of the detection performance as the ambient temperature changes from -40 to 125 ^{circ}C. The temperature coefficient (TC) for R_S is chosen as a nominal values from off the shelf resistors as $200ppm/°C$. The TC for R_{SCA} was selected as $100ppm/°C$. V_{thresh} was set to a constant 496 mV off-chip regardless of temperature. Since the variation in R_S with temperature moves the common-mode voltage $(\mu_0 + \mu_1)/2$ but V_{thresh} stays constant, TP reduces with temperature steadily as $\phi(\frac{V_{thresh}-\mu_1}{\sigma_{out}})$ reduces. TN has negligible improvement since $FP = \phi(\frac{V_{thresh}-\mu_0}{\sigma_{out}})$ is close to 0% already. Any further increase in $\mu_0 - V_{thresh}$ helps little in boosting up TN.

C. On PPA Overhead

Fig. 16 shows the layout of a test chip implementing the proposed P-SCA detection circuit. The excitation and measurement systems occupy $0.015mm^2$ and $0.008mm^2$ respectively.

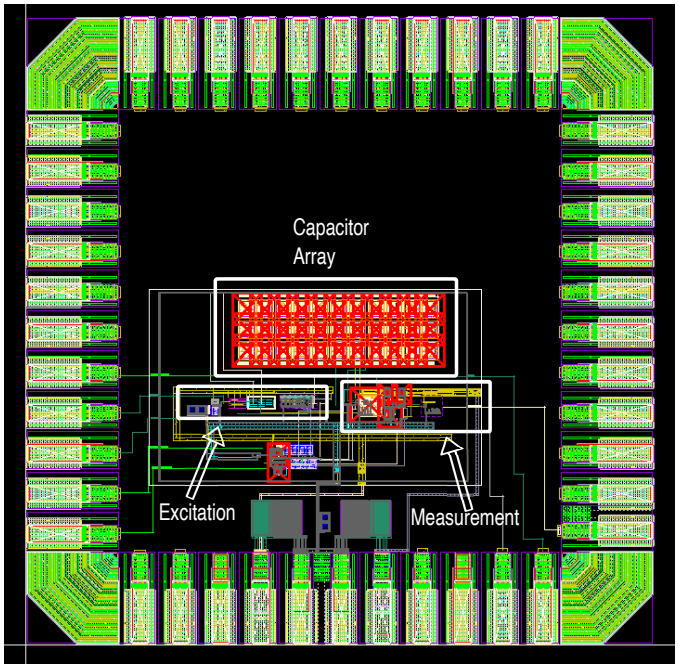

Fig. 16. Proposed circuits implemented in a 65nm CMOS test chip

31 pF of C_S and C_F occupy $0.033mm^2$, as shown in the middle of the test chip. Clock generation circuit layout area is not included in the area overhead count, as it can often be shared with other on-board circuits. The total quiescent current (I_Q) of the excitation system is 19.33 μA. I_Q for the measurement system is 16.87 μA. These absolute power and area overhead can be converted to relative overheads if the baseline SoC die size and power consumption is assumed.

Compared to machine learning based [11], [12] P-SCA detection methods, the circuit does not present any training time, epoch, or data size overhead for users. Compared to algorithm-based side-channel attack protections, such as masking [34], the proposed circuits do not present any performance overhead to the encryption engine they seek to protect. This feature is shared by other P-SCA detection circuits.

VII. Conclusion

This paper presents the first analyses on the fundamental limit and performance tradeoffs of generic and energy-efficient DC resistance (DCR) based power side-channel trojan detection circuits. This paper found the minimal detectable resistance to be a function of the circuit's thermal noise and the desired statistical significance of the detection. With this knowledge, designers can predict the detection performance from specifications before any transistor design. This paper illustrated that environmental factors, such as temperature, supply impedance, and supply voltage, appear as common-mode signals. Hence, they do not affect detection performance in the first order. Simulations results from IC blocks designed in a 65-nm CMOS process confirmed the above analyses.

REFERENCES

[1] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Advances in Cryptology — CRYPTO' 99*, M. Wiener, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, pp. 388–397.

[2] N. Miura, D. Fujimoto, D. Tanaka, Y.-i. Hayashi, N. Homma, T. Aoki, and M. Nagata, "A local EM-analysis attack resistant cryptographic engine with fully-digital oscillator-based tamper-access sensor," in *Symp. VLSI circuits Tech. Dig.* IEEE, 2014, pp. 1–2.

[3] P.-C. Liu, H.-C. Chang, and C.-Y. Lee, "A true random-based differential power analysis countermeasure circuit for an AES engine," *IEEE Trans. Circuits Syst. II: Exp. Briefs*, vol. 59, no. 2, pp. 103–107, 2012. [Online]. Available: https://dx.doi.org/10.1109/TCSII.2011.2180094

[4] F. Macé, F.-X. Standaert, I. Hassoune, J.-D. Legat, J.-J. Quisquater *et al.*, "A dynamic current mode logic to counteract power analysis attacks," in *Proc. 19th Int. Conf. on Design of Circuits and Integr. Syst. (DCIS)*, 2004, pp. 186–191.

[5] H. Mestiri, F. Kahri, B. Bouallegue, and M. Machhout, "A CPA attack against cryptographic hardware implementation on SASEBO-GII," in *2017 Int. Conf. on Green Energy Conversion Systems (GECS)*, 2017, pp. 1–5.

[6] K. Tiri, M. Akmal, and I. Verbauwhede, "A dynamic and differential CMOS logic with signal independent power consumption to withstand differential power analysis on smart cards," in *Proc. 28th European Solid-State Circuits Conf.*, 2002, pp. 403–406.

[7] D. Das, J. Danial, A. Golder, N. Modak, S. Maity, B. Chatterjee, D. Seo, M. Chang, A. Varna, H. Krishnamurthy *et al.*, "27.3 EM and Power SCA-resilient AES-256 in 65nm CMOS Through $>350\times$ Current-Domain Signature Attenuation," in *2020 IEEE Int. Solid-State Circuits Conference - (ISSCC)*. IEEE, 2020, pp. 424–426.

[8] D. Das, S. Maity, S. B. Nasir, S. Ghosh, A. Raychowdhury, and S. Sen, "ASNI: Attenuated signature noise injection for low-overhead power side-channel attack immunity," *IEEE Trans. Circuits Syst. I: Reg. Papers*, vol. 65, no. 10, pp. 3300–3311, 2018.

[9] A. Singh, M. Kar, S. K. Mathew, A. Rajan, V. De, and S. Mukhopadhyay, "Improved power/EM side-channel attack resistance of 128-bit AES engines with random fast voltage dithering," *IEEE J. Solid-State Circuits*, vol. 54, no. 2, pp. 569–583, 2018.

[10] H. Wang, H. Sayadi, S. Rafatirad, A. Sasan, and H. Homayoun, "Scarf: Detecting side-channel attacks at real-time using low-level hardware features," in *2020 IEEE 26th Int. Symp. On-Line Testing and Robust System Design (IOLTS)*. IEEE, 2020, pp. 1–6.

[11] D. Utyamishev and I. Partin-Vaisband, "Real-time detection of power analysis attacks by machine learning of power supply variations on-chip," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 39, no. 1, pp. 45–55, 2020.

[12] F. Kenarangi and I. Partin-Vaisband, "Exploiting machine learning against on-chip power analysis attacks: Tradeoffs and design considerations," *IEEE Trans. Circuits Syst. I: Reg. Papers*, vol. 66, no. 2, pp. 769–781, 2019.

[13] N. Gattu, M. N. I. Khan, A. De, and S. Ghosh, "Power side channel attack analysis and detection," in *2020 IEEE/ACM Int. Conf. Computer Aided Design (ICCAD)*, Nov 2020, pp. 1–7.

[14] N. Kaushik and J. Hu, "A switched-capacitor power side-channel attack detection circuit in 65-nm CMOS," in *2020 IEEE Int. Symp. Circuits Syst. (ISCAS)*, May 2021.

[15] R. Munny and J. Hu, "Power side-channel attack detection through battery impedance monitoring," in *2020 IEEE Int. Symp. Circuits Syst. (ISCAS)*, May 2021.

[16] D. A. Johns and K. Martin, *Analog integrated circuit design*. John Wiley & Sons, 2008.

[17] J. N. Y. Aziz, K. Abdelhalim, R. Shulyzki, R. Genov, B. L. Bardakjian, M. Derchansky, D. Serletis, and P. L. Carlen, "256-channel neural recording and delta compression microsystem with 3d electrodes," *IEEE J. Solid-State Circuits*, vol. 44, no. 3, pp. 995–1005, 2009.

[18] S. J. Kim, S. H. Han, J. H. Cha, L. Liu, L. Yao, Y. Gao, and M. Je, "A sub-μW/Ch analog front-end for Δ-neural recording with spike-driven data compression," *IEEE Trans. Biomed. Circuits Syst.*, vol. 13, no. 1, pp. 1–14, 2019.

[19] C. C. Enz and G. C. Temes, "Circuit techniques for reducing the effects of op-amp imperfections: autozeroing, correlated double sampling, and chopper stabilization," *Proc. IEEE*, vol. 84, no. 11, pp. 1584–1614, 1996.

[20] B. Murmann, "Thermal noise in track-and-hold circuits: Analysis and simulation techniques," *IEEE Solid State Circuits Mag.*, vol. 4, no. 2, pp. 46–54, 2012.

[21] "Z score table," http://www.z-table.com/, May 2021, [Online; accessed 12-May-2021].

[22] M. Sokolova and G. Lapalme, "A systematic analysis of performance measures for classification tasks," *Information Processing & Management*, vol. 45, no. 4, pp. 427–437, 2009. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0306457309000259

[23] D. Chicco and G. Jurman, "The advantages of the matthews correlation coefficient (MCC) over F1 score and accuracy in binary classification evaluation," *BMC genomics*, vol. 21, no. 1, pp. 1–13, 2020.

[24] M. Burns, G. W. Roberts *et al.*, *An introduction to mixed-signal IC test and measurement*. IET, 2001, vol. 2001.

[25] H. Zhu, R. Kapusta, and Y.-B. Kim, "Noise reduction technique through bandwidth switching for switched-capacitor amplifier," *IEEE Trans. Circuits Syst. I: Reg. Papers*, vol. 62, no. 7, pp. 1707–1715, 2015.

[26] B. Hershberg, S. Weaver, K. Sobue, S. Takeuchi, K. Hamashita, and U. Moon, "Ring amplifiers for switched capacitor circuits," *IEEE J. Solid-State Circuits*, vol. 47, no. 12, pp. 2928–2942, 2012.

[27] Y. Lim and M. P. Flynn, "A 1 mw 71.5 db sndr 50 ms/s 13 bit fully differential ring amplifier based sar-assisted pipeline adc," *IEEE J. Solid-State Circuits*, vol. 50, no. 12, pp. 2901–2911, 2015.

[28] E. Iroaga and B. Murmann, "A 12-bit 75-ms/s pipelined adc using incomplete settling," *IEEE J. Solid-State Circuits*, vol. 42, no. 4, pp. 748–756, 2007.

[29] F. van der Goes, C. M. Ward, S. Astgimath, H. Yan, J. Riley, Z. Zeng, J. Mulder, S. Wang, and K. Bult, "A 1.5 mw 68 db sndr 80 ms/s 2\ $times$ interleaved pipelined sar adc in 28 nm cmos," *IEEE J. Solid-State Circuits*, vol. 49, no. 12, pp. 2835–2845, 2014.

[30] X. Tang, X. Yang, W. Zhao, C.-K. Hsu, J. Liu, L. Shen, A. Mukherjee, W. Shi, S. Li, D. Z. Pan *et al.*, "A 13.5-enob, 107-μw noise-shaping sar adc with pvt-robust closed-loop dynamic amplifier," *IEEE J. Solid-State Circuits*, vol. 55, no. 12, pp. 3248–3259, 2020.

[31] P. Harpe, E. Cantatore, and A. Van Roermund, "A 10b/12b 40 ks/s sar adc with data-driven noise reduction achieving up to 10.1 b enob at 2.2 fj/conversion-step," *IEEE J. Solid-State Circuits*, vol. 48, no. 12, pp. 3011–3018, 2013.

[32] H. S. Bindra, C. E. Lokin, D. Schinkel, A. Annema, and B. Nauta, "A 1.2-v dynamic bias latch-type comparator in 65-nm CMOS with 0.4-mv input noise," *IEEE J. Solid-State Circuits*, vol. 53, no. 7, pp. 1902–1912, 2018.

[33] B. Razavi, "The design of a comparator [the analog mind]," *IEEE Solid State Circuits Mag.*, vol. 12, no. 4, pp. 8–14, 2020.

[34] W. Yu and S. Köse, "A lightweight masked aes implementation for securing iot against cpa attacks," *IEEE Trans. Circuits Syst. I: Reg. Papers*, vol. 64, no. 11, pp. 2934–2944, 2017.