Analysis and Design of CMOS Integrated Power Side-Channel Attack Detection Circuits

Nipun Kaushik, *Student Member, IEEE,* John Hu, *Senior Member, IEEE*

***Abstract*—Power side-channel attacks (PSCA) are hardware-level cyberattacks that are highly effective in data breaches but very difficult to detect. The difficulty is due to their passive nature and noninvasiveness to the victim. Recent work on a switched-capacitor (SC) based power side-channel attack (PSCA) detection presents a more generic and computation-efficient method than prior arts. However, the performance limitation and design tradeoffs for this new method remain unknown. This paper presents the first complete mathematical analysis and simulations that seek to guide future designs for CMOS integrated power side-channel attack (PSCA) detection circuit. The minimum detectable resistance is shown to be proportional to circuit noise and desired detection confidence while inversely proportional to the excitation current. Aided by this insight, a first circuit reduced the PSCA detection voltage sensitivity by 33x (from 2.5 mV to 75 μV) and energy per detection by 2.2x (2000 pJ to 925 pJ). The second circuit applied delta modulation to mitigate true negative (TN) degradation from 4.5x to 1.7x across the entire range of R_s variations. Both circuits were designed in a general-purpose 65 nm CMOS process consuming 130 μW and occupy approximately 0.055 mm^2.**

***Index Terms*—Hardware security, power side-channel attack detection, CMOS integrated circuit, circuit noise**

I. Introduction

HARDWARE security of microelectronics has received growing attention due to their importance to every day life from consumer electronics to military applications. In the cyber world, attacks that exploits hardware vulnerability is on the rise. Power analysis side-channel attacks, or PSCAs, is one such attacks that is very effective in data breach.

Research shows the relation between side channel information and the information being guarded. The information can exist on side channels such as power consumption [1]–[3], electromagnetic emanations [4]–[6],thermal signatures [7]–[9],optical [10], [11], timing [12], [13] and acoustic [14], [15]. Since the discovery of side-channel attacks (SCA), various countermeasures have been proposed.

Logic-level countermeasures have been proposed to make devices more secure. Wave dynamic differential logic (WDDL) proposed in Advanced Encryption Standard (AES) achieves a Minimum Traces to Disclosure (MTD) of 1.5 million against correlational power analysis (CPA) based SCA [16]. False key and lightweight masking-based countermeasure improved the MTD to above 150 million [17]. Circuit-level countermeasures have also been proposed to enhance security with less power and area overhead. Digital LDOs were proposed in addition to random noise injection to attenuate the current signature from AES engine, attaining MTD above 1 billion traces [18], [19]. Random fast voltage tethering (RFVD) randomized the control loop to improve MTD and TVLA benchmarks [20]. Both types of countermeasure aimed to increase the MTD with minimal power, performance, and area overhead.

All the countermeasures mentioned above follow a *one-size-fit-all* approach. However, the same countermeasure may be too costly in terms of power consumption for some environments and provide insufficient protection in other settings. What if chips can sense their side-channel attack threats and adjust their counter- measures accordingly? The benefits would be clear – chips can obtain security under various conditions and consume just the right amount of power and overhead. The feasibility for adaptive countermeasures hinges on one challenge: how to sense and detect side channel attacks in real time. This lead to work in *proactive* power [21]–[25] and EM [26], [27] SCA detection methods. A thorough review of these work will be presented in Section II.

Detecting power side-channel attacks (PSCA) is hard problem. Its challenge comes from the attacks being passive and non-intrusive to the victim. Despite the number of work proposed, the performance limitation and design tradeoffs that would affect low-cost, integrated power side-channel attack detection circuit designs remain unknown. This paper seeks to analyze the fundamental relationships between the detection accuracy and circuit-level parameters to guide future design of PSCA detection ICs.

The rest of the paper is as follows. A threat model is discussed in section II, which describes the scope of detection and conditions for a PSCA. Section III describes the detection scheme and circuits used for detection. The performance analysis and trade-offs are discussed in section IV. Section V goes through the measurement and simulation results of the proposed technique.A discussion is presented in section VI, which covers appropriateness and limits of the threat model. Section VII concludes this paper.

II. Threat Model and Previous Research

A. PSCA Threat Model

Fig. 1 shows the power side-channel attack (PSCA) threat model we will investigate in this paper. The adversary aims to extract the encryption keys from the victim IC, which contains a cryptographic engine. The hacker can measure the victim's power consumption by inserting a current sensing resistor, R_{attack} [28]. The voltage drop across R_{attack} is captured by an oscilloscope (or other data acquisition devices) and sent to a PC for power analysis.

N. Kaushik and J. Hu are with the School of Electrical and Computer Engineering, Oklahoma State University, Stillwater, OK, 74078 USA e-mail: nipun.kaushik@okstate.edu.

Manuscript received Feb 25, 2021.

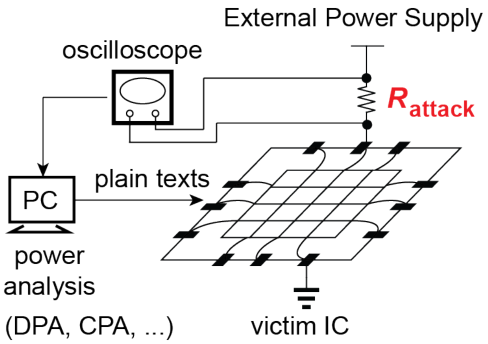

Fig. 1: Power Side-Channel Attack (PSCA) Threat Model

This threat model is consistent with previous research [21], [22]. Some prior work [23] further specify that R_{attack} will be inserted via modifying one of the many package V_{DD} pins. The victim IC then exploits this asymmetry for PSCA detection [23]. In this paper, we refrain from making assumptions on where and how the R_{attack} is inserted. Our goal is to make our detection method generic and applicable to a wide range of R_{attack} insertion scenarios. As such, our detection circuit would offer maximum security benefit.

B. Previous Research on PSCA Detection

Real-time on-chip PSCA detection was first proposed in [21]. The threat model assumed is the same as Fig. 1. They derived the closed-form expression for the on-chip power distribution network (PDN) voltage variations caused by the malicious R_{attack}. On-chip voltage sensors then sense the whole PDN and feed the data into a machine learning algorithm for PSCA detection. Their follow-up work [22] further studied the optimum sensor distribution to achieve full chip coverage. The advantage of this approach is that it is generic and applies to a wide variety of R_{attack} insertion locations. The limitations, however, have to do with the large number of voltages that need to sensed for classification. The number of sensors needed for sufficient coverage and the resolution required for classification make the method data and power intensive.

A more energy-efficient PSCA detection method was proposed in [23]. It assumed that the R_{attack} was inserted by removing a single V_{DD} package ball and replace it with a surface-mount resistor. It also assumed that there were other V_{DD} balls that are unaltered. This package modification will create an on-chip voltage imbalance ΔV between these pins. The attack can then be detected by comparing the victim node voltage with its neighboring attack-free nodes. Inverter-based Ring Oscillators (RO) were further used to convert voltage into frequency and let the detection be based on frequency comparisons. The advantage of this work is the energy-efficiency and quick detection time due to the use of ROs. The drawback is the assumption that R_{attack} would only affect one V_{DD} node but leave other V_{DD} nodes intact somehow narrow the detection scope. As the authors acknowledged, if the R_{attack} was inserted on the PCB between the voltage regulator module (VRM) and the victim IC, all the V_{DD} pins would be affected by the IR-drop equally. An on-chip ΔV would not exist for detection.

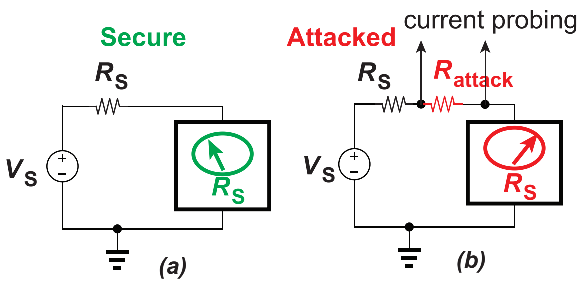

Fig. 2: Detection Method: An on-chip Thevenin equivalent resistance (R_s) sensor can differentiate between (a) secure configuration (b) attacked configuration. The attacked configuration has unexpected high R_s value.

In summary, real-time PSCA detection research is still in its infancy. Generic and energy-efficient detection circuits that are amiable for on-chip integration is highly desirable.

III. Proposed Detection System and Circuits

A. Proposed Detection Method

Fig. 2 shows the proposed detection method. An *unexpected* supply resistance *increase* will be considered as a power side-channel attack (PSCA) incident. This is because no matter where the attacker inserts the shunt resistor (R_{attack}), the Thevenin equivalent impedance (R_s) looking into the external source will increase. Hence, the PSCA detection problem is translated into the design of an on-chip R_s sensor. If the sensed R_s increases unexpected, a PSCA must have taken place due to an R_{attack} insertion. The proposed method have several advantages over prior arts [21]–[23].

(1) Only one physical attribute (R_s) needs to be measured. Compared to [21], [22] that needs to measure all PDN voltages, data size, sensor numbers, and overall power consumption should be greatly reduced.

(2) Explainability of the detection method. Compared to supervised Machine Learning (ML) models [21], [22], the proposed R_s-based detection can be as simple as a threshold comparison. Human users can comprehend and trust the detection results as much as they trust the threat model and the R_s measurement accuracy. This explainability helps us reveal its performance limitations and tradeoffs later in Section IV.

(3) Wide detection scope. Compared to [23], no assumption is made about the manner of the insertion or the presence of an on-chip ΔV. Hence, it can detect the cases (e.g., R_{attack} inserted on the PCB between VRM and the IC) that [23] cannot.

B. Architecture of the R_s Sensor

Integrated impedance (or resistance) sensors exist in many biomedical [29]–[31] and industrial applications [32]. For example, bio-impedance (BIOZ) readout ICs have been designed for vital signal measurement [29], Electrical Impedance Tomography [30], and personal health monitoring [31]. However,

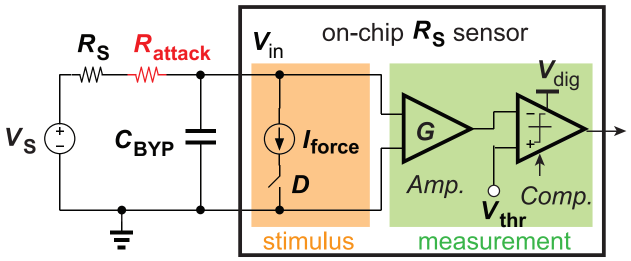

Fig. 3: Block diagram for the on-chip R_s sensor consisting of a current stimulus module (orange) and a voltage measurement (green) module

many such sensor's architecture are not suitable for the PSCA detection application. because of the following reasons:

(1) Active vs. passive. For BIOZ and infrastructure fault monitoring, the biomedical tissue or the physical infrastructure is a passive element. Hence, stimulus current can flow in both directions. For PSCA detection, the power source is an active circuit that may only allow current in one direction.

(2) Common-mode voltage. For passive measurands, the DC voltage at which the impedance is measured can be defined by the sensor IC to maximize the signal swing. For PSCA detection, the common-mode voltage cannot be defined. It is either VDD or ground. Sensing R_s at supply rails may present difficulties in level shifting and dynamic range.

Considering these challenges, Fig. 3 shows the proposed architecture of the R_s sensor for PSCA detection. It consists of two modules – stimulus and measurement. The stimulus module is a pulsed current source with duty cycle D and current magnitude I_{force}. The measurement module consists of a voltage amplifier followed by a comparator. The decision to use current as stimulus and voltage as response is consistent with most other integrated impedance sensors [29]–[31]. It is driven by the wide availability of current sink and voltage amplifier intellectual properties (IP) on mixed-signal ICs. As I_{force} is periodically turned on, if we ignore all the other load current on the victim chip, V_{in} would experience a commensurate, periodical voltage drop ΔV. The Thevenin equivalent series resistance R_s can be calculated as:

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

Alternative impedance sensing topologies exist, but they are not chosen due to their complexity. For example, sinusoidal and pseudo-sinusoidal current stimulus can be used for the current stimulus generation. However, they require oscillators with frequency selection network [33] or multi-bit digital-to-analog converters (DAC) with adaptive quantization look-up table [34], which require significant design effort. Similarly, synchronous demodulation could be used to measure resistance and reactance [29], [31] or magnitude and phase [35], [36]. However, since the PSCA detection is interested in the *change* of R_s, not the absolute value of R_s itself, these topologies were foregone for the simpler solution shown in Fig. 3.

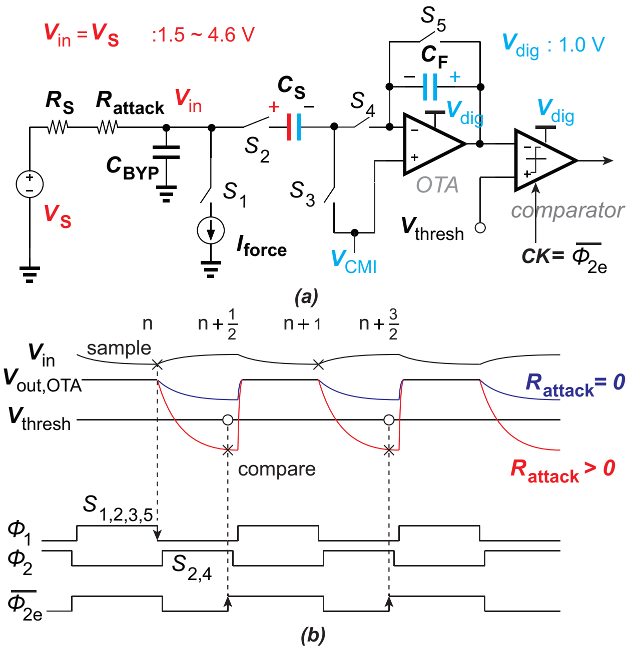

Fig. 4: Switched-capacitor PSCA detection circuits (a) voltage amplification and comparison (b) non-overlapping clock for bottom-plate sampling and comparison

C. Circuit Implementation

Fig. shows a discrete-time switched-capacitor implementation of the on-chip R_s sensor circuit [24]. The stimulus module consists of switch S_1 and a current sink. The measurement module includes a CMOS track-and-hold amplifier (THA) and a comparator. The THA circuit accomplishes delta modulation, level shifting, and low-noise amplification (LNA). The delta modulation (Δ-mod.) can be understood as follows [37].

(1) During phase 1 (ϕ_1), switches $S_{1,2,3,5}$ are closed. The current I_{force} causes V_{in} to drop below V_s. The final value is sampled by C_S: $V_{in}[n] = V_s - I_{force}(R_S + R_{attack})$.

(2) During phase 2 (ϕ_2), switches $S_{2,4}$ are closed, and $S_{1,3,5}$ are open. Since I_{force} is removed when S_1 opens, V_{in} bounces back to V_s: $V_{in}[n + \frac{1}{2}] = V_s$.

(3) C_S, C_F, and the output transconductance amplifier (OTA) form the CMOS THA circuit. The charge sampled by C_S by the end of ϕ_1 will be redistributed with C_F during ϕ_2. If we omit the DC common-mode voltage of the THA (i.e., V_{CMI}) and focus on the AC output voltage v_{out}:

$$\begin{aligned} v_{out}[n + \frac{1}{2}] &= -\frac{C_S}{C_F}(v_{in}[n + \frac{1}{2}] - v_{in}[n]) \\ &= -\frac{C_S}{C_F} I_{force}(R_S + R_{attack}) \end{aligned} \tag{2}$$

From Eq. 2, we can see that the CMOS THA realizes a Δ-mod. on the input voltage V_{in} between time $[n + \frac{1}{2}]$ and $[n]$. The Thevenin equivalent voltage V_s is cancelled as a common-mode voltage. The remaining signal is an amplified version of $I_{force} {\cdot} R_s$, or $I_{force} {\cdot} (R_s + R_{attack})$ if there is an attack present. Hence, this voltage ($v_{out}[n + \frac{1}{2}]$) can be compared against a pre-determined threshold (V_{thresh}) for PSCA detection.

TABLE I: Definition of the Confusion Matrix Elements

Truth	Detected as PSCA (1)	Detected as Secure (0)
PSCA (1)	True Positive (TP)	False Negative (FN)
Secure (0)	False Positive (FP)	True Negative (TN)

The switched-capacitor circuit also achieves level shifting through C_s. C_s is implemented using a high voltage tolerant metal-insulator-metal (MIM) capacitor. The top plate (red) faces the input V_{in}. The bottom plate (blue) is switched between the input common-mode voltage (V_{CMI}) and the virtual ground (also V_{CMI}). As such, the OTA and comparator can be designed using core transistors under digital supply voltage $V_{dig} = 1V$. This helps reduce the dynamic power consumption of those circuits.

IV. Performance Analysis and Tradeoffs

The detection performance of the proposed circuits can be evaluated using similar benchmarks as other cyberattack detection or binary classification circuits. The evaluation metrics include accuracy, detection time, sensitivity, and overhead. However, the proposed circuits also have unique physical-level property and detection performance tradeoffs. We will derive these tradeoffs in this section and show their relevance in PSCA detection IC design.

A. Performance Metrics

1) Accuracy: Similar to other binary classification tasks, the confusing matrix $M = \begin{pmatrix} TP & FN \\ FP & TN \end{pmatrix}$ [38] can evaluate the accuracy of a PSCA detection system. In this paper, we use 0 or negative to refer to a truly safe condition. We use 1 or positive to refer to electronics that are currently under a PSCA attack. The definition of each element of M in the PSCA detection context is defined in Table I.

Next, this paper formulates the problem of PSCA detection as **Hypothesis testing**. We assume that all devices operate in a safe and PSCA-free condition by default (a.k.a. null hypothesis: H_0.) Through monitoring the change in the Thenevin equivalent resistance R_s, the proposed circuits seek to reject H_0 with high statistical significance (α, β).

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

The significance level α is the probability of making a Type-I error, i.e., rejecting H_0 when the device is actually secure. α is also equal to the False Positive (FP) rate in the confusion matrix. Similarly, β is the probability of making a Type-II error, which is failing to reject H_0 when a PSCA is present. β is equal to the False Negative (FN) rate in Table I.

2) Detection Time: PSCA detection is most valuable if the detection circuits can generate decisions before a PSCA completes. Different countermeasures can then be deployed to prevent further information leakage. For the same detection accuracy and statistical significance, it is desirable to obtain PSCA detection results quicker so that more time can be allocated for reactive countermeasures. In this paper, the detection time can be defined as:

$$t_{DET} = t_1 - t_0 \tag{3}$$

t_0 indicates the time when a PSCA is launched by the attacker. t_1 is the time when the PSCA detection circuit generate a positive or negative result. Many PSCA detection circuits operate on a duty cycle basis [24], [39], it may be more insightful to characterize the average of t_{DET} as $E(t_{DET}) = E(t_1) - t_0$. $E(\cdot)$ is the mean of a random variable.

3) Sensitivity: Not every resistor value that an attacker uses can be detected by the proposed circuits. Larger R_{attack} will create a large voltage signal ($v_{out}[n + \frac{1}{2}]$ in Eq. 2) that can be exploited for fast and reliable PSCA detection. Small R_{attack} may generate a voltage that is indistinguishable from noise despite the amplification. Similar to the study of RF transceiver, we define *sensitivity* as the minimal detectable attack resistor R_{min} that can be detected with a given statistical significance (α, β). It is reasonable to expect that as the tolerable α, β reduces, the R_{min} would increase, meaning that it is generally harder to detect the intrusion of a small resistor than a large one with the same confidence.

4) Overhead: Like any other ASIC functionality, it is necessary to quantify the power, performance, and area (PPA) overhead for a new feature. Comparison of PPA overhead is always tricky because the same hardware functionally may incur different PPA cost in different CMOS processes, and the scaling of the PPA overhead across nodes may not be linear. Nevertheless, quiescent current (I_Q), energy per detection (E), power consumption during detection (P), total capacitance (pF) and die area (mm^2) remain useful metrics for overhead comparison. Machine learning solutions [21], [22] may incur additional overhead in data collection and model training. The proposed solution [24] will also need V_{thresh} determination based on empirical data or analytical studies.

B. Sensitivity, Noise, and Accuracy Tradeoff

Sensitivity of the proposed PSCA detection system will be affected by circuit noise. This is similar to the sensitivity of an wireless transceiver (P_{sen}), which is determined by the noise figure, bandwidth, and minimum SNR requirement [40]. This section will derive a close-form expression for R_{min}, which will be determined by input-referred noise, current stimulus, and minimum accuracy requirement [41]

Fig. 5 shows the basis for our sensitivity derivation. Our detection circuits are based on resistance measurements. Since resistance measurement involves uncertainty, we assume that the measured R_s under the secure and attacked scenario both follow a Gaussian distribution. Let X_0 and X_1 be the random variable representing the final settled under both cases. $X_0 \sim \mathcal{N}(r_0, \sigma_0)$, $X_1 \sim \mathcal{N}(r_1, \sigma_1)$. Since the R_s is measured using the same circuit regardless of the attack status, we assume $\sigma_0 = \sigma_1 = \sigma = u(R_s)$. $u(R_s)$ represents the total measurement uncertainty of R_s according to the GUM [42]. From Fig. 5, there is a minimum number of σ's r_0 and r_1 need to be separated so that a threshold r_{th} can be selected to achieve low α and β rates simultaneously. We denote this minimum number of σ that r_0 and r_1 needs to be separated as $f(\alpha, \beta)$. $f(\alpha, \beta)$ can be found as follows:

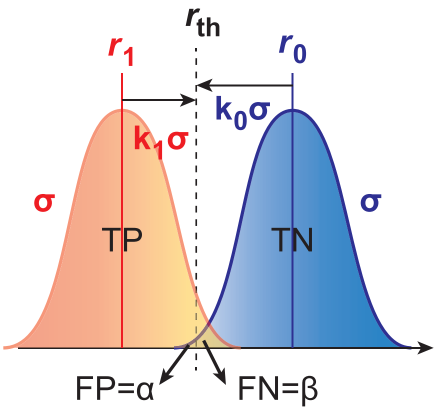

Fig. 5: Sensitivity derivation. If $|r_1 - r_0| \geq f(\alpha,\beta)\sigma$, then there exists a r_{th} that can meet accuracy requirements.

TABLE II: Typical $f(\alpha,\beta)$ Values for different FP,FN targets

FP (α)	FN (β)	k_0	k_1	$f(\alpha,\beta)$
0.05	0.05	1.65	1.65	3.29
0.05	0.01	1.65	2.33	3.98
0.01	0.05	1.65	2.33	3.98
0.01	0.01	2.33	2.33	4.66

$$\because |r_0 - r_1| = |r_0 - r_{th}| + |r_{th} - r_1| = k_0\sigma + k_1\sigma$$
$$\therefore f(\alpha,\beta) = k_0 + k_1 \tag{4}$$

k_0 and k_1 can be found be looking up the Z-table or numerically by solving Eq. 5 and 6. Table II shows some of the typical $f(\alpha,\beta)$ values based on different combinations of 1% to 5% FP, FN tolerance.

$$Z(k_0) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{k_0} e^{-\frac{x^2}{2}} dx = 1 - \alpha \tag{5}$$
$$Z(k_1) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{k_1} e^{-\frac{x^2}{2}} dx = 1 - \beta \tag{6}$$

Next, we apply this analysis to the block diagram in Fig. 3. In this paper, we assume I_{force} will not contribute to $u(R_s)$ because it can be trimmed to be within one LSB of the design target on the Automatic Test Equipment (ATE). The LSB for current measurement on mainstream ATE is on the order of $1\mu A$. Even if there is $\pm 50\%$ uncertainty on the ATE LSB, $u(I_{force}) = 0.5\mu A$ would only lead to $u(V_{in}) = 0.5\mu V_{rms}$ (if $R_{attack} = 1\Omega$), which is much smaller than typical voltage measurement noise and error. As the PSCA detection system tries to detect even smaller R_{attack}, the voltage uncertainty will dominate $u(R_s)$.

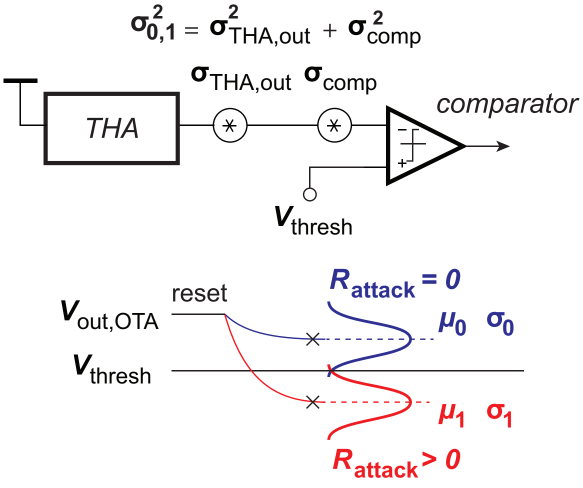

Fig. 6: Noise model in the voltage measurement circuits

Finally, we analyze how noise contributes to voltage measurement uncertainty in our proposed circuits in Fig. 4 (a). Fig. 6 shows its noise mode. The output noise of the CMOS THA ($\sigma_{THA,out}$) and the comparator input-referred noise (σ_{comp}) add uncertainty to the comparator decision. For ease of analysis, we lump both noises together at comparator's negative input ($\sigma_{0,1}$) so the comparator and the threshold voltage V_{thresh} appear noise free. Since the two noise sources are from different circuits and are uncorrelated, we can express the lumped noise for secure and attacked configuration as:

$$\sigma^2_{0,1} = \sigma^2_{THA,out} + \sigma^2_{comp} \tag{7}$$
$$= \sqrt{\sigma^2_{THA,in} \cdot G^2 + \sigma^2_{comp}} \tag{8}$$

The THA gain is $G = C_S/C_F$, and the subscript 0 and 1 corresponds to the secure and attacked cases, respectively. The mean values at the THA output in Fig. 6 (ignoring the common reset voltage) for both configurations are:

$$\mu_0 = G \cdot \Delta V = G \cdot I_{force} R_s \tag{9}$$
$$\mu_1 = G \cdot \Delta V' = G \cdot I_{force}(R_s + R_{attack}) \tag{10}$$

Based on previous analysis, in order to pick a V_{thresh} that can meet the requirement ($FP < \alpha$, $FN < \beta$) simultaneously, μ_0 and μ_1 should be separated by $f(\alpha,\beta) \cdot \sigma_{0,1}$:

$$|\mu_0 - \mu_1| \geq f(\alpha,\beta) \cdot \sigma_{0,1} \tag{11}$$

Replace μ_0 and μ_1 with their expressions (Eq. 9 and 10):

$$G \cdot I_{force} R_{attack} \geq f(\alpha,\beta)\sigma_{0,1} \tag{12}$$
$$\therefore R_{attack} \geq \frac{f(\alpha,\beta)\sigma_{0,1}}{G \cdot I_{force}} \tag{13}$$

Eq. 13 indicates that there is a minimum detectable R_{attack} (R_{min}) for any pair of (α,β) requirement. If we plug in the lumped noise $\sigma_{0,1}$ for our proposed circuit (Eq. 8):

$$R_{min} = \frac{f(\alpha,\beta)}{I_{force}} \cdot \sqrt{\sigma^2_{THA,in} + \frac{\sigma^2_{comp}}{G^2}} \tag{14}$$
$$= \frac{f(\alpha,\beta) \cdot \sigma_{in}}{I_{force}} \tag{15}$$

Eq. 15 shows the sensitivity, accuracy, and noise tradeoff. This equation matches the qualitative analysis in Section

IV.A.(3): (1) Sensitivity is inversely proportional to noise, or $R_{min} \propto \sigma_{in}$. (2) Sensitivity is inversely proportional to detection confidence level, or $R_{min} \propto f(\alpha, \beta)$. (3) Sensitivity is inversely proportional to I_{force}, or $R_{min} \propto 1/I_{force}$. This is consistent with other studies [39]. Increasing I_{force}, however, comes at the cost of extra power consumption.

C. Mitigation of Benign Variations

Even if we can measure R_s with high certainty (e.g., thanks to a low-noise design with $\sigma_{in} \approx 0$), this does not automatically make the circuit proposed in Fig. 4 an ideal PSCA detector. The change in R_s could very likely be coming from benign variations, such as temperature or process-induced changes in R_s. This can be understood by looking at Fig. 6. As R_s varies, the mean values for μ_0 and μ_1 would shift up or down. If a fixed V_{thresh} is used for PSCA detection, then either TP or TN rates would deteriorate under such variations.

To mitigate the benign variation, the distance between μ_0 and μ_1 should be used for detection, as suggested in Eq. 11. However, the circuit in Fig. 4 did not implement Eq. 11. Instead, the circuit compared the absolute value of $v_{out}[n+\frac{1}{2}]$ with V_{thresh}. Therefore, an improved version of the PSCA detection circuit can be designed that subtracts $v_{out}[n+\frac{1}{2}]$ from $v_{out}[n+\frac{3}{2}]$.

To account for the benign variation of R_s over time, we can model R_s as a as a time series $R_s[n]$. Since the victim does not know when and if R_{attack} will be inserted, we can also model R_{attack} as a time series, $R_{attack}[n]$. A second delta modulator at the THA output can generate the following time series $y[n]$:

$$\begin{aligned} y_{out}[n+\frac{3}{2}] &= v_{out}[n+\frac{3}{2}] - v_{out}[n+\frac{1}{2}] \\ &= G \cdot I_{force}(R_{attack}[n+1] - R_{attack}[n]) \quad (16) \end{aligned}$$

Here, Eq. 16 assumes that temperature (T) and manufacturing-induced R_S changes happen much slower than a clocking period, i.e., $R_s[n+1] \approx R_s[n]$. But the attack resistor is assumed to be inserted at a random instance. Between the two clock cycles that R_{attack} was inserted, $R_{attack}[n+1] - R_{attack}[n] = R_{attack} - 0 = R_{attack}$.

Fig. 7 shows an improved PSCA detection circuit the implements the operation of Eq. 16. Three additional clock phases are introduced to implement two sampling and a subtraction operation. During ϕ_3, the THA output $v_{out}[n+\frac{1}{2}]$ is sampled on $C_{H,1}$. During ϕ_4, $v_{out}[n+\frac{3}{2}]$ is sampled on $C_{H,2}$. Both ϕ_3 and ϕ_4 are derived from ϕ_2 so that they are non-overlapping to ϕ_1. Φ_5 is derived from every other ϕ_1. At the rising edge of ϕ_5, $C_{H,2}$ are stacked on top of $C_{H,1}$. But the reverse polarity ensures that the input voltage seen at the comparator negative input is $v_{out}[n+\frac{3}{2}] - v_{out}[n+\frac{1}{2}$. A threshold voltage V'_{thresh} is used to set the proper PSCA detection trigger. Notice this V'_{thresh} is different from the V_{thresh} in Fig. 4. It can be manually tuned to be around $\frac{1}{2}G \cdot I_{force}R_{attack,0}$ for a balanced TP and TN performance. Here $R_{attack,0}$ is the anticipated R_{attack} that will be used by the adversary.

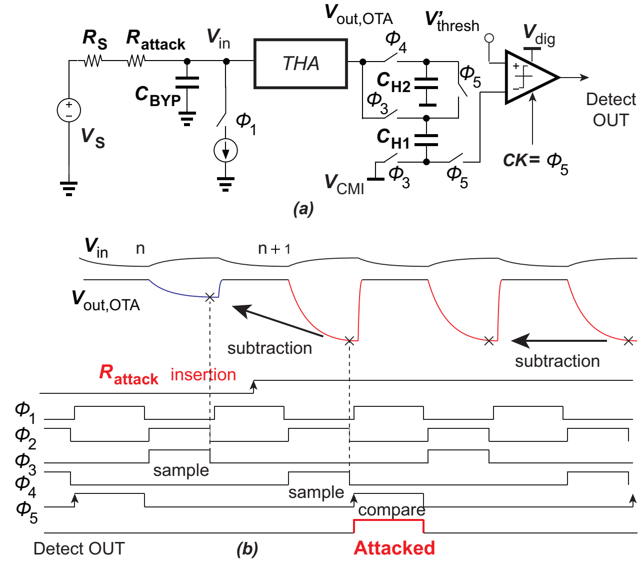

Fig. 7: Improved PSCA detection circuits with R_s cancellation (a) additional delta modulation at the THA output to cancel R_s (b) timing and clock waveforms

There are several advantages of the improved circuit in Fig. 7. First, it is robust to R_s variations, as R_s changes are being cancelled like a common-mode signal ($R_{attack}[n+1] - R_{attack}[n] \approx 0$.) Together with the inherent supply rejection coming from Section III.C: Eq. 2, the detection performance will be robust amidst to board-to-board and supply-to-supply variations. Second, the detection threshold V'_{thesh} has a clear physical meaning. For example, if the victim would like to sense a very small R_{attack}, it can set V'_{thesh} as close to the common-mode voltage V_{CMI} as possible, since the anticipated spike due to R_{attack} insertion is well-defined as $G \cdot I_{force}R_{attack}$. Thirdly, V'_{thresh} can also be fine tuned to remove the input offset of the comparator. The V_{thresh} in Fig. 4 cannot conveniently do so because the actual value of μ_0 and μ_1 would depend on R_s, which may change from source to source.

The disadvantage, however, is that the R_{attack} insertion would generate only a single pulse, as shown in red in Fig. 7. Having a single pulse as the detection output may have certain disadvantages. If for whatever reason the subsequent detection circuit misses this pulse, there will be no additional alarms to indicate the attacker's presence. The original circuit in Fig. 4, on the other hand, would continue to generate positive detection outputs as long as $v_{out}[n+\frac{k}{2}]$ crosses V_{thresh} ($k = 1, 2, \cdots, \infty$) after the attacker insertion.

V. Simulation and Measurement Results

The original and improved PSCA detection circuits (Fig. 4 and 7) were designed in TSMC 65 nm General Purpose CMOS process. The OTA used in Fig. 4 and 7 is an NMOS input two-stage operational amplifier [43] with total $I_Q = 21\mu A$ and unity gain frequency (UGF) of 10 MHz. This was designed to satisfy the settling requirements in the switched-capacitor circuit given a moderate close-loop gain and the resulting small feedback factor ($C_S/C_F = 30, \beta = 1/30$.) The maximum

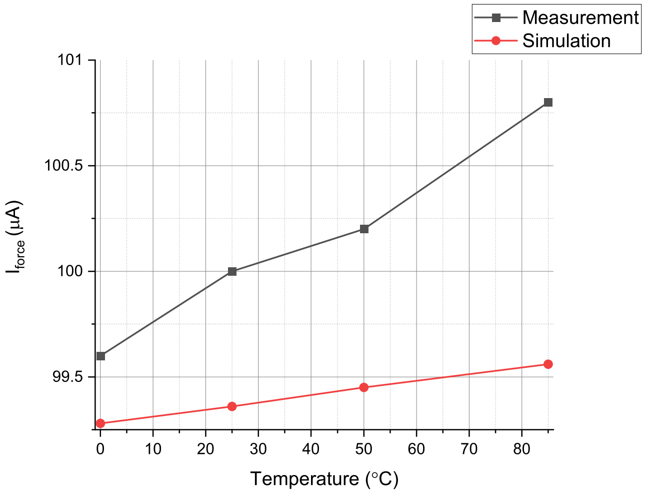

Fig. 8: Variation of I_{force} with temperature

speed for the PSCA detection was limited to 200 kHz. This limit was set due to the external RC time constant if a typical bypass capacitor of $0.47\mu F$ is used to filter supply noise. The nominal supply impedance was assumed to $150m\Omega$, as it approximates the sum of the internal battery resistance of a single-cell Li-Ion battery and well designed PCB that minimize supply routing resistance.

The comparator used in in Fig. 4 and 7 are the dynamic comparator proposed in [44], which dynamically reduces the input-referred thermal noise and minimize power loss by preventing internal nodes' full discharge to ground. The I_{force} was implemented using the basic cascode current mirror for better accuracy. Its nominal output is $100\mu A$. All circuit components in Fig. 4 were fabricated in a CLCC 44-pin test chip. The accuracy of the I_{force} current over temperature was simulated and measured on the silicon to verify some basic assumptions made in this paper.

A. Variation of Excitation Current I_{force}

The variation of I_{force} with temperature is an important metric to define the threshold. Figure 8 shows the variation of excitation current with temperature from 0 °C to 85 °C. The ideal desired value of the excitation current is 100 µ. The simulated version of the design performs consistently across the range. Lab measurement verifies the performance of excitation current. The variation acts as threshold for detection as $I_{force}.(R_s+R_sns)$. The current variation can translate into false errors and lower detection accuracy. From Fig. 8, we can see that the assumption in Section IV.B that I_{force} will not contribute much to the uncertainty of R_s is well founded. The maximum error from silicon is less than $1\mu A$ from from 0 °C to 85 °C. Part of the reason this current was stable is because the I_{ref} for the cascode current mirror was generated off-chip using an ideal voltage source and a high temperature stability resistor.

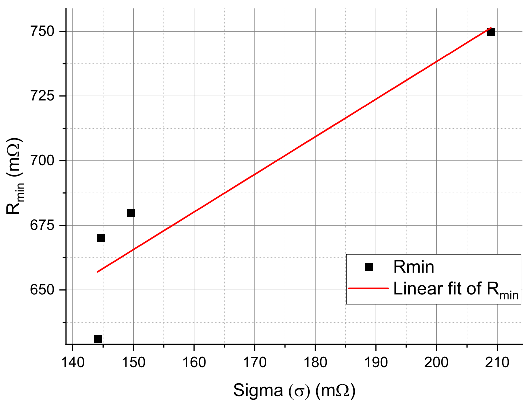

Fig. 9: Relation of Rmin and Sigma in a linear curve

B. Verification of Sensitivity, Noise, and Accuracy Tradeoff

Fig. 9 shows the linear relationship between R_{min} and σ_{in}. For the circuit in Fig. 4, the input-referred noise is determined once the voltage measurement circuits were designed. It is hard to vary σ_{in} without changing the bias current and power consumption. In this paper, we choose to scale σ_{in} through majority vote averaging. If the PSCA detection were repeated N times, and the final result was based on a majority vote, the input-referred thermal noise should be scaled by $\sigma_{scale} = \frac{\sigma_{in}}{\sqrt{N}}$.

We then simulate the circuit in Fig. 4 to find the corresponding R_{min} under each σ_{scale}. The circuit without averaging results in a higher sigma leading to a high R_{min}. Majority voting reduces the σ which enables detection of lower R_{min}. This is consistent with the theory developed for increasing detection range by decreasing the σ.Sigma can be reduced to a certain limit by averaging. Decrease in σ by averaging more number of times get limited by the offset and non-idealities of the system. There is a point which shows the saturation of sigma. The sigma(144mΩ) does not decrease any further by increasing the majority voting from N=9 to N=16. The circuit without any modification starts from 208 mΩ which can be thought of as an upper rail. The lower rail is lowest achievable sigma by attained by averaging. This defines the limits for R_{min} sensing based on noise and the supporting theory.

C. Performance under Benign Variations

Fig 10 shows the variation of accuracy with the variation of the power supply for the original PSCA detection circuit in Fig. 4. Low error rates ensure successful detection during the operation. This circuit is capable of working across a wide range of battery voltage. The switched capacitor uses delta modulation to sample the V_{BAT} each period. The figure shows a confusion matrix based on 598 samples. The accuracy of the system is consistent and high across the range. This makes the topology independent of power supply variation.

Fig. 11 shows the detection accuracy variation when R_s is changed from -50% to +500% of the nominal value ($150m\Omega$). For the original circuit in Fig. 4, the TP value approaches

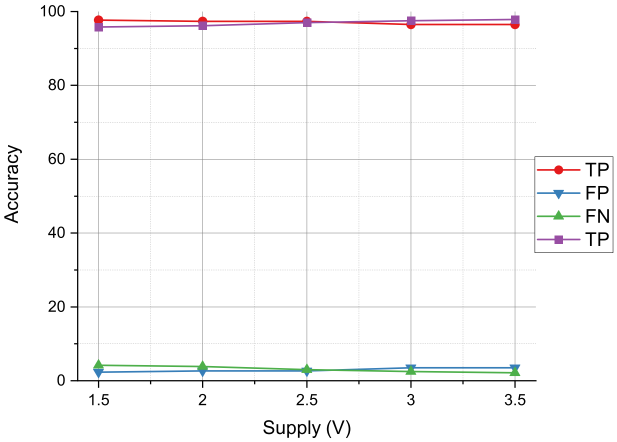

Fig. 10: Accuracy with variation of Power supply

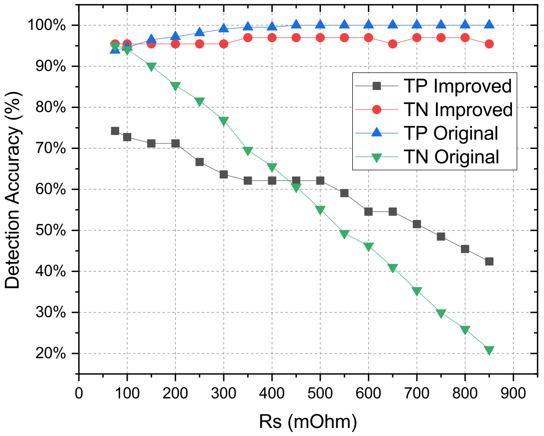

Fig. 11: Variation of Detection Accuracy Under R_s Variations

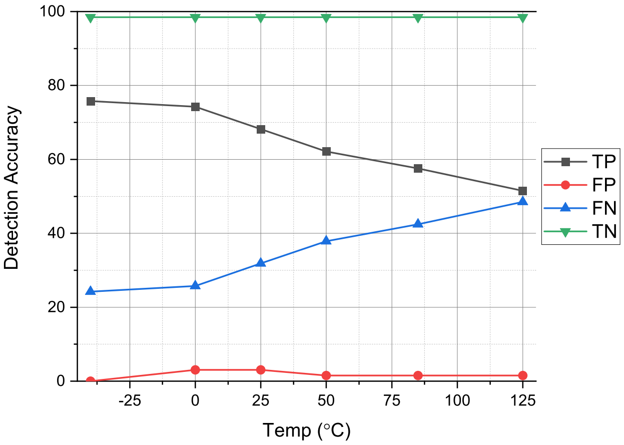

Fig. 12: Variation of Detection Accuracy of the Improved Circuit in Fig. 7 Under Temperature Variation

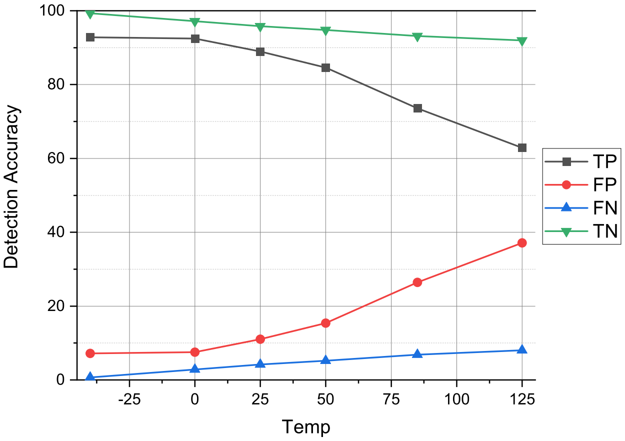

Fig. 13: Variation of Detection Accuracy of the Original Circuit in Fig. 4 Under Temperature Variation

100% as R_s exceeds $300m\Omega$, but this came at the price of TN degrading from 95% from $75m\Omega$ to 20% at $850m\Omega$. This 4.5x drop in accuracy is due to keeping the same V_{thresh} as μ_0 continually shifts downward as R_s increases (Fig. 6). For the improved circuit in Fig. 7, the TN stays relatively constant across the whole R_s variation range. The TP degrades from 74% to 42%, but this 1.7x degradation is less than 4.5x drop in the original. The TP does not stay perfectly flat probably due to the non-idealities from the switching activities in the second delta mod. circuit and non-perfect cancellation of R_s.

However, the R_s cancellation has only limited effectiveness against temperature variations. Under ambient temperature variation, not only will R_s change, the R_{attack} used by the adversary may change value, too. Fig. 12 shows the improved circuit's accuracy under temperature change from $0°C$ to $85°C$. It is interesting to compare it with the temperature induced changes in the original circuit shown in Fig. 13. Both circuits have accuracy degradation as the temperature increases. This is expected as σ_{in} generally increases with temperature, and the R_{attack} and R_s assumed 100 ppm/$°C$ and 0.00393 to model a typical current sense resistor and PCB copper trace Temperature Coefficient, respectively. The subtle difference is that Fig. 13 shows that both TP and FP reduces, which is consistent with the depiction in Fig. 6 where V_{thresh} is stationary but σ_0 and σ_1 increases. Fig. 12 shows the detection for H_0 (secure configuration) relatively unchanged but H_1 (attacked) degrading. The detection for H_0 is probably a false impression because as $G \cdot I_{force} R_{attack}$ moves further lower than V'_{thresh}, the comparator is harder to generate a positive pulse under any circumstance. Thus, this bias made TN and FP appear constant and immune to σ increase.

D. Detection of R_s

Figure 14 shows the detection of sense resistor by the track and hold circuit. R_s is inserted at 100μs, which changes the response of the OTA. This before and after difference decides

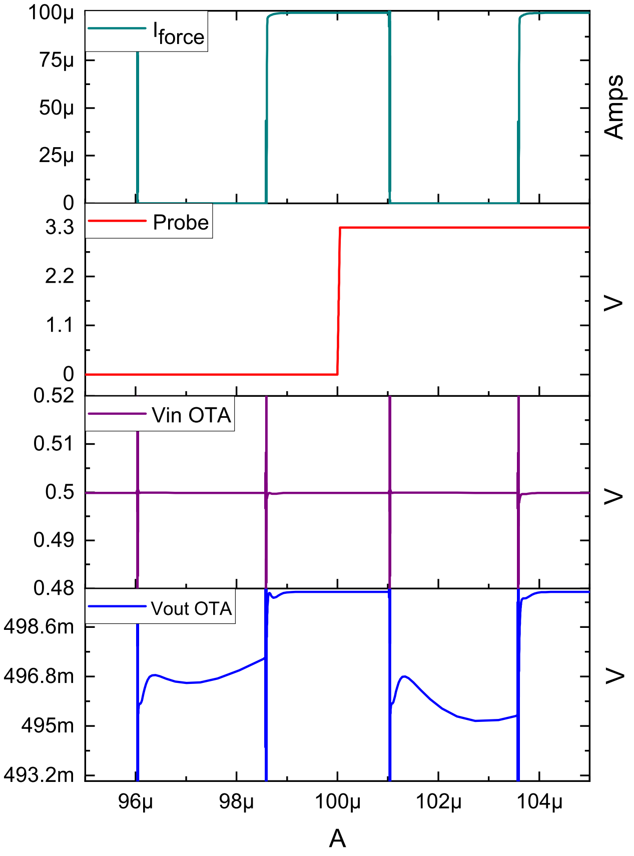

Fig. 14: Output of OTA with insertion of sense resistor R_s

the threshold of the system. If the voltage after insertion is close to the threshold voltage, it creates false detections. More variation after insertion leads to fewer error rates. The magnitude of the output after insertion depends on the gain of track and hold topology. This circuit is designed for a gain of 30V/V and it leads to a change based on $(R_s+R_{attack})\cdot I_{force}$

E. Noise simulations

Figure 15 shows the transient noise at the output of OTA. This is a critical node for circuit performance. It goes to the input of comparator and a decision is made based on the threshold. The comparator threshold voltage is compared to the moving transient signal which can lead to errors.

Figure 16 shows the distribution of noise at the output of OTA. The noise at OTA output is a prime factor in deciding the threshold of the comparator. The detection of R_{attack} is affected by the distribution of noise. Overlapping regions of sigma lead to false detections. Reducing the sigma for different configurations (safe and attack) decreases error rates. The mean of the distribution acts as a threshold.

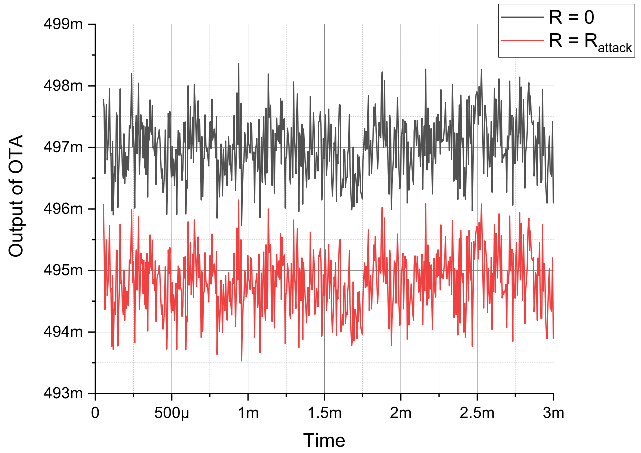

Fig. 15: Transient noise at the output of OTA

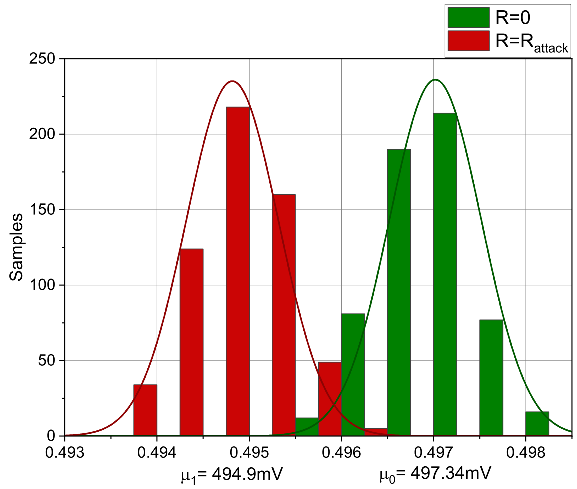

Fig. 16: Noise distribution at the output of OTA

The chip was fabricated in 65 nm CMOS technology. Figure 17 shows the layout view before fabrication. It shows major blocks including the capacitor array for a switched-capacitor sample and hold circuit. The excitation block includes the current array, and reference generation circuits. Sensitive analog circuitry is placed away from the clock generation circuit. The OTA and comparator are placed close to the output. A 44 pin CLCC package is used for these chips.

VI. Discussions

The threat model in Fig. 1 may seem to have limitations. For instance, adversaries may probe the victim IC's power consumption differently, such as using an inductive current probe or a Source Measure Unit (SMU) (a test equipment that can source and measure at the same time [45].) However, an inductive current probe is an EM probe. Thus, EM SCA detection methods [26], [27] can detect their presence. An SMU also has its internal impedance, R_s'. Since R_s' is probably different from what the victim expects as safe R_s, our method would still detect SMU-based probing. Thus, the R_{attack}-based threat model in Fig. 1 represents the majority of low-cost PSCA efforts. [21]–[23], [39]. Our proposed circuits will make

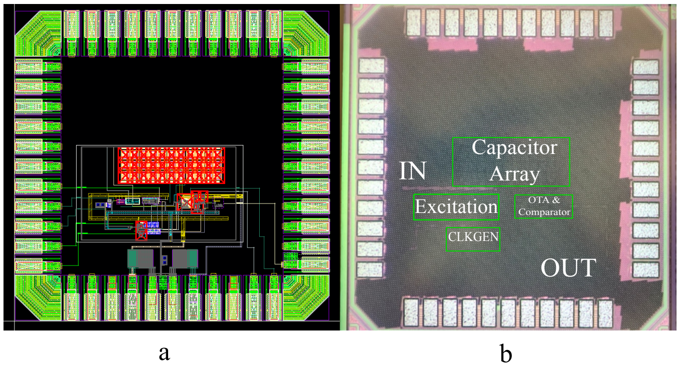

Fig. 17: Comparison of layout view and the taped out chip a) Layout view b) Die photo

TABLE III: Comparison with other work

	This work	[24]	[39]	[23]	[21]	Units
Process	65		65	22	45	nm
R_{min}	0.6	N.A	0.1∼50	1	N.A	Ω
V_{min}	60	N.A	2500	N/A	3900	µV
Detection method	R_s sensing		R_s sensing	ΔV sensing	PDN sensing	NA
Sensors	1		1	≥2	30	NA
R@pin	YES		YES	NO	YES	NA
R@PCB	YES		YES	NO	YES	NA
E/det	925	12177	2000	200	2000	pJ
R_{min}	0.75	NA	0.1 to 50	<1	1	Ω
V_{min}	75	NA	2500	N.A.	3900^A	µV
Area	0.055	0.35	0.028	N.R	0.091	mm^2
I_{force}	0.1	10	0.4∼20	N.A.	N.A	mA
t_{det}	5	4.1	NR	2	0.394-30	μs
Accuracy	95%	NA	100%	N.A.	88%	%

A: Estimated based on 8-bit ADC with 1V Vref

these low-cost attacks futile. Prospective hackers will have to create new, more elaborate methods to probe power or current, which will raise their cost and time and nullify their incentives to launch PSCAs.

VII. Conclusion

This paper presents the first complete analysis and design for CMOS integrated power side-channel attack (PSCA) detection circuit. The detection is based on sensing unexpected changes in the external supply's Thevenin equivalent resistance (R_s). The minimum detectable resistance is shown to be proportional to circuit noise and desired detection confidence while inversely proportional to the excitation current. Driven by this insight, two PSCA detection circuits were designed. The first one reduced the voltage sensitivity by 33x (from 2.5 mV to $75\mu V$) and energy per detection by 2.2x (2000 pJ to 925 pJ) by targeting 95% detection accuracy and avoid over-designs. The second one leverages a basic delta modulation circuit that reduced the True Negative (TN) degradation from 4.5x to 1.7x across the entire range of R_s variations. Both circuits consume round 130 μW with an active area of 0.055 mm^2.

References

[1] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Annual international cryptology conference*. Springer, 1999, pp. 388–397.

[2] S. Mangard, E. Oswald, and T. Popp, *Power analysis attacks: Revealing the secrets of smart cards*. Springer Science & Business Media, 2008, vol. 31.

[3] M. Randolph and W. Diehl, "Power side-channel attack analysis: A review of 20 years of study for the layman," *Cryptography*, vol. 4, no. 2, p. 15, 2020.

[4] D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi, "The em side—channel (s)," in *International workshop on cryptographic hardware and embedded systems*. Springer, 2002, pp. 29–45.

[5] K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic analysis: Concrete results," in *International workshop on cryptographic hardware and embedded systems*. Springer, 2001, pp. 251–261.

[6] J. Longo, E. De Mulder, D. Page, and M. Tunstall, "Soc it to em: electromagnetic side-channel attacks on a complex system-on-chip," in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2015, pp. 620–640.

[7] P. Gu, D. Stow, R. Barnes, E. Kursun, and Y. Xie, "Thermal-aware 3d design for side-channel information leakage," in *2016 IEEE 34th International Conference on Computer Design (ICCD)*. IEEE, 2016, pp. 520–527.

[8] M. Hutter and J.-M. Schmidt, "The temperature side channel and heating fault attacks," in *International Conference on Smart Card Research and Advanced Applications*. Springer, 2013, pp. 219–235.

[9] R. J. Masti, D. Rai, A. Ranganathan, C. Müller, L. Thiele, and S. Capkun, "Thermal covert channels on multi-core platforms," in *24th {USENIX} Security Symposium ({USENIX} Security 15)*, 2015, pp. 865–880.

[10] J. Ferrigno and M. Hlaváč, "When aes blinks: introducing optical side channel," *IET Information Security*, vol. 2, no. 3, pp. 94–98, 2008.

[11] F. Stellari, A. Tosi, F. Zappa, and S. Cova, "Cmos circuit analysis with luminescence measurements and simulations," in *32nd European Solid-State Device Research Conference*. Citeseer, 2002, pp. 495–498.

[12] D. Brumley and D. Boneh, "Remote timing attacks are practical," *Computer Networks*, vol. 48, no. 5, pp. 701–716, 2005.

[13] P. C. Kocher, "Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems," in *Annual International Cryptology Conference*. Springer, 1996, pp. 104–113.

[14] E. Toreini, B. Randell, and F. Hao, "An acoustic side channel attack on enigma," *School of Computing Science Technical Report Series*, 2015.

[15] M. E. Smid and D. K. Branstad, "Data encryption standard: past and future," *Proceedings of the IEEE*, vol. 76, no. 5, pp. 550–559, 1988.

[16] K. Tiri, D. Hwang, A. Hodjat, B.-C. Lai, S. Yang, P. Schaumont, and I. Verbauwhede, "Prototype ic with wddl and differential routing–dpa resistance assessment," in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2005, pp. 354–365.

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

[18] 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.

[19] A. Ghosh, D. Das, J. Danial, V. De, S. Ghosh, and S. Sen, "36.2 an em/power sca-resilient aes-256 with synthesizable signature attenuation using digital-friendly current source and ro-bleed-based integrated local feedback and global switched-mode control," in *2021 IEEE International Solid- State Circuits Conference (ISSCC)*, vol. 64, 2021, pp. 499–501.

[20] 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.

[21] 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.

[22] 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.

[23] N. Gattu, M. N. Imtiaz Khan, A. De, and S. Ghosh, "Power side channel attack analysis and detection," in *2020 IEEE/ACM Int. Conf. Comput. Aided Design ICCAD*, 2020, pp. 1–7.

[24] N. Kaushik and J. Hu, "A Switched-Capacitor Power Side-Channel Attack Detection Circuit in 65-nm CMOS," in *2021 IEEE International Symposium on Circuits and Systems (ISCAS)*, May 2021, pp. 1–5.

[25] R. Munny and J. Hu, "Power Side-Channel Attack Detection through Battery Impedance Monitoring," in *2021 IEEE International Symposium on Circuits and Systems (ISCAS)*, May 2021, pp. 1–5.

[26] D.-H. Seo, M. Nath, D. Das, B. Chatterjee, S. Ghosh, and S. Sen, "PG-CAS: Patterned-Ground Co-Planar Capacitive Asymmetry Sensing for mm-Range EM Side-Channel Attack Probe Detection," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, May 2021, pp. 1–5.

[27] 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 *2014 Symp. VLSI Circuits Dig. Tech. Papers*, Jun. 2014, pp. 1–2.

[28] G. Goodwill, B. Jun, J. Jaffe, and P. Rohatgi, "A testing methodology for side-channel resistance validation," in *NIST non-invasive attack testing workshop*, vol. 7, 2011, pp. 115–136.

[29] H. Ha, W. Sijbers, R. Van Wegberg, J. Xu, M. Konijnenburg, P. Vis, A. Breeschoten, S. Song, C. Van Hoof, and N. V. Helleputte, "A Bio-Impedance Readout IC With Digital-Assisted Baseline Cancellation for Two-Electrode Measurement," *IEEE J. Solid-State Circuits*, vol. 54, no. 11, pp. 2969–2979, Nov. 2019.

[30] M. Kim, J. Jang, H. Kim, J. Lee, J. Lee, J. Lee, K.-R. Lee, K. Kim, Y. Lee, K. J. Lee, and H.-J. Yoo, "A 1.4-mΩ -Sensitivity 94-dB Dynamic-Range Electrical Impedance Tomography SoC and 48-Channel Hub-SoC for 3-D Lung Ventilation Monitoring System," *IEEE J. Solid-State Circuits*, vol. 52, no. 11, pp. 2829–2842, Nov. 2017.

[31] N. Van Helleputte, M. Konijnenburg, J. Pettine, D.-W. Jee, H. Kim, A. Morgado, R. Van Wegberg, T. Torfs, R. Mohan, A. Breeschoten, H. de Groot, C. Van Hoof, and R. F. Yazicioglu, "A 345 µW Multi-Sensor Biomedical SoC With Bio-Impedance, 3-Channel ECG, Motion Artifact Reduction, and Integrated DSP," *IEEE J. Solid-State Circuits*, vol. 50, no. 1, pp. 230–244, Jan. 2015.

[32] Y. Hu, W. S. A. Rieutort-Louis, J. Sanz-Robinson, L. Huang, B. Glišic, J. C. Sturm, S. Wagner, and N. Verma, "Large-scale sensing system combining large-area electronics and cmos ics for structural-health monitoring," *IEEE J. Solid-State Circuits*, vol. 49, no. 2, pp. 513–523, 2014.

[33] L. Yan, J. Pettine, S. Mitra, S. Kim, D.-W. Jee, H. Kim, M. Osawa, Y. Harada, K. Tamiya, C. Van Hoof, and R. F. Yazicioglu, "A 13 $\mu \rm A$ Analog Signal Processing IC for Accurate Recognition of Multiple Intra-Cardiac Signals," *IEEE Trans. Biomed. Circuits Syst.*, vol. 7, no. 6, pp. 785–795, Dec. 2013.

[34] S. Kim, L. Yan, S. Mitra, M. Osawa, Y. Harada, K. Tamiya, C. van Hoof, and R. F. Yazicioglu, "A 20µW intra-cardiac signal-processing IC with 82dB bio-impedance measurement dynamic range and analog feature extraction for ventricular fibrillation detection," in *2013 IEEE ISSCC Dig. Tech. Papers*, Feb. 2013, pp. 302–303.

[35] M. Zamani, Y. Rezaeiyan, O. Shoaei, and W. A. Serdijn, "A 1.55 µW Bio-Impedance Measurement System for Implantable Cardiac Pacemakers in 0.18 µm CMOS," *IEEE Trans. Biomed. Circuits Syst.*, vol. 12, no. 1, pp. 211–221, Feb. 2018.

[36] K. Kim, J.-H. Kim, S. Gweon, M. Kim, and H.-J. Yoo, "A 0.5-V Sub-10-μW 15.28-m$\Omega/\sqrt{Hz}$ Bio-Impedance Sensor IC With Sub-1°C Phase Error," *IEEE J. Solid-State Circuits*, vol. 55, no. 8, pp. 2161–2173, Aug. 2020.

[37] 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, Mar. 2009.

[38] 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

[39] S. J. Kim, D. Kim, A. Sharma, and M. Seok, "EQZ-LDO: A Near-Zero EDP Overhead, gt;10M-Attack-Resilient, Secure Digital LDO featuring Attack-Detection and Detection-Driven Protection for a Correlation-Power-Analysis-Resilient IoT Device," in *Proc. 2021 Symp. VLSI Circuits*, Jun. 2021, pp. 1–2.

[40] B. Razavi and R. Behzad, *RF microelectronics*. Prentice hall New York, 2012, vol. 2.

[41] N. Kaushik and J. Hu, "Performance and Noise Trade-off for SC-based Power Side-Channel Attack Detection Circuits," in *2021 IEEE International Midwest Symposium on Circuits and Systems (MWSCAS)*, Aug. 2021, pp. 770–773.

[42] *Guide to the Expression of Uncertainty in Measurement (GUM)*, 2008, gUM 1995 with minor corrections. [Online]. Available: https://www.bipm.org/documents/20126/2071204/JCGM_100_2008_E.pdf/cb0ef43f-baa5-11cf-3f85-4dcd86f77bd6

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

[44] 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.

[45] *SMU Selector Guide*, Tektronics, Aug. 2021. [Online]. Available: https://www.tek.com/en/documents/product-selector-guide/source-measure-unit-smu-instruments-selector-guide

Nipun Kaushik (Student Member, IEEE) received the B.Tech degree in electronics and communication from Kurukshetra University, Panipat, India, in 2014. He received his M.S in electrical engineering from The University of Texas, Arlington in 2017. He is a second-year Ph.D. student at Oklahoma State University. He worked as an analog-mixed signal intern at Synaptics, San Jose, CA as a member of the mobile silicon team in summer 2021. His research interest includes analog, mixed-signal design, and hardware security integrated circuit design. He served as a session chair for Midwest IEEE International Midwest Symposium on Circuits and Systems (MWSCAS) in 2021.

John Hu (Senior Member, IEEE) received the B.S. degree in electronics and information engineering from Beihang University, Beijing, China, in 2006, and the M.S. and Ph.D. degrees in electrical and computer engineering from the Ohio State University, Columbus, OH, in 2007 and 2010, respectively. Between 2011 and 2012, he was an analog IC designer at Texas Instruments, Dallas, TX. From 2012 to 2016, he was a Member of Technical Staff, IC Design at Mobility Business Unit of Maxim Integrated, San Diego, CA. Between 2016 and 2019, he was a Staff Engineer at Qualcomm in Tempe, AZ. In August 2019, he joined the School of Electrical and Computer Engineering at Oklahoma State University as an assistant professor. His research interests include analog, mixed-signal, power management, and hardware security integrated circuit design in CMOS technologies. He was a visiting faculty at the Air Force Research Lab, Cyber Assurance Branch, in summer 2021. He has served as an Associate Editor on Frontiers in Electronics and conference session chairs for IEEE International Midwest Symposium on Circuits and Systems (MWSCAS) and IEEE International Microwave Symposium (IMS). He is a working group member of the Oklahoma Semiconductor Alliance and holds 3 U.S. patents.