IEEE Open Journal of the
Solid-State Circuits Society

Received 18 November 2024; revised 26 March 2025; accepted 7 May 2025. Date of publication 19 May 2025; date of current version 17 June 2025.

Digital Object Identifier 10.1109/OJSSCS.2025.3571334

R-STELLAR: A Resilient Synthesizable Signature Attenuation SCA Protection on AES-256 With Built-In Attack-on-Countermeasure Detection

ARCHISMAN GHOSH [1] (Graduate Student Member, IEEE), DONG-HYUN SEO [2], DEBAYAN DAS [3] (Member, IEEE), SANTOSH GHOSH [4] (Member, IEEE), AND SHREYAS SEN [1] (Senior Member, IEEE)

[1]IC Design, Ixana, West Lafayette, IN 47906, USA
[2]RFIC Design Group, SK Hynix, Icheon-si, South Korea
[3]Department of Electrical Engineering, Indian Institute of Science, Bengaluru 560012, India
[4]GPU HW Engineering, Nvidia, Hillsboro, OR 97006, USA

CORRESPONDING AUTHORS: A. GHOSH and S. SEN (e-mail: ghosh69@purdue.edu; shreyas@purdue.edu)

This work was supported in part by NSF under Grant CNS 17-19235, and in part by the Intel Corporation.

ABSTRACT Side-channel attacks (SCAs) remain a significant threat to the security of cryptographic systems in modern embedded devices. Even mathematically secure cryptographic algorithms, when implemented in hardware, inadvertently leak information through physical side-channel signatures, such as power consumption, electromagnetic (EM) radiation, light emissions, and acoustic emanations. Exploiting these side channels significantly reduces the attacker's search space. In recent years, physical countermeasures have significantly increased the minimum traces-to-disclosure (MTD) to 1 billion. Among them, signature attenuation is the first method to achieve this mark. Signature attenuation often relies on analog techniques, and digital signature attenuation reduces MTD to 20 million, requiring additional methods for high resilience. We focus on improving the digital signature attenuation by an order of magnitude (MTD 200M). Additionally, we explore possible attacks against signature attenuation countermeasure. We introduce a voltage-drop linear-region biasing (VLB) attack technique that reduces the MTD to over 2000 times less than the previous threshold. This is the first known attack against a physical SCA countermeasure. We have implemented an attack detector with a response time of 0.8 ms to detect such attacks, limiting the SCA leakage window to sub-ms, which is insufficient for a successful attack.

INDEX TERMS AES-256, correlational power analysis, electromagnetic (EM) leakage, generic countermeasure, hardware security, side-channel attacks (SCAs), synthesizable signature attenuation, test vector leakage assessment (TVLA).

I. INTRODUCTION

CRYPTOGRAPHIC algorithms are designed to be secure based on mathematical principles. However, they can unintentionally reveal sensitive side-channel information. This type of leakage typically happens due to power correlations, electromagnetic (EM) emissions, timing, and variations in cache accesses. Such leaks are a serious security risk for integrated circuits (ICs). Theoretically, AES-256 can be broken with a brute-force attack, requiring 2^{256} trials to deterministically steal the AES key. However, side-channel attack (SCA) has reduced the minimum traces-to-disclosure (MTD) to approximately 2^{13}. This implies that storing 2^{13} power traces could be used to extract the entire key, thereby reducing the attack complexity to 2^{13} [1]. Recent observations reveal that the AES-256 key can be intercepted even from a distance using a low-cost EM probe without detailed knowledge of the circuit or PCB implementation [2]. An adversary monitors the information to exploit this leakage and correlates it against a statistical model constructed using secret key guesses. Correlation attacks utilize Hamming

weight (HW) or Hamming distance (HD) models to estimate the switching activities of internal nodes within a cryptographic engine. Depending on the strength of the underlying power model and the availability of power signatures, a correct key guess yields correlation peaks, revealing portions of the secret key. An alternative analysis for evaluating side-channel vulnerabilities in crypto hardware is the test vector leakage assessment (TVLA) [18]. This analysis estimates model-independent information leakage by applying Welch's $|t|$-test to a set of fixed and random plaintext vectors. If the resulting $|t|$-score exceeds a heuristic threshold of 4.5, the device is considered to exhibit meaningful leakage.

The research community has been exploring various countermeasures in response to the emergence of SCAs. Architectural countermeasures involve heterogeneous S-boxes, arithmetic masking, and multiplicative masking. These methods aim to enhance security by introducing complexity and obfuscation at the architectural level. In contrast, generic and physical countermeasures address vulnerabilities at the physical implementation level. Examples include randomized series low-dropout (LDO) regulators as well as analog and digital signature attenuation circuits (DSACs). Some countermeasures combine multiple approaches to achieve robust protection against side-channel leakage. Our work focuses on a high-attenuation technique based on a digitally *cascoded* current source (CS), leveraging a single generic approach. Security remains a dynamic challenge akin to a cat-and-mouse game. Attackers have questioned the efficacy of certain architectural countermeasures under specific circumstances. However, attacks against physical countermeasures remain unexplored. We successfully explored an attack on a physical countermeasure for the first time. Contributions of this work are threefold, as shown in Fig. 1.

1) We introduce a signature attenuation technique using a digital cascoded CS (DCCS), namely, resilient signature attenuation embedded crypto with low-level metal routing (R-STELLAR). This countermeasure could not be attacked with 200M power traces which is 20× greater than existing single, physical, generic countermeasure (≈10M traces) requiring at least 20 times more time to extract AES key with respect to current solutions. Moreover, this could be integrated with other solutions for more benefit.
2) Additionally, we explore an attack, namely, voltage-drop linear-region biasing attack (VLB) on physical countermeasures, significantly reducing MTD from 200 million traces to 105K traces.
3) Finally, we propose an attack detection mechanism crucial for the practical adoption of physical countermeasures in industry.

The subsequent sections of this article are structured as follows. In Section II, we delve into related research on countermeasures against power and EM SCA, along with potential vulnerabilities. Section III provides an in-depth analysis of the circuit architecture. In Section IV, we outline the proposed attack strategy and its corresponding mitigation technique. Section V presents the measurement setup, results, and IC specifications. Finally, we conclude this article in Section VI.

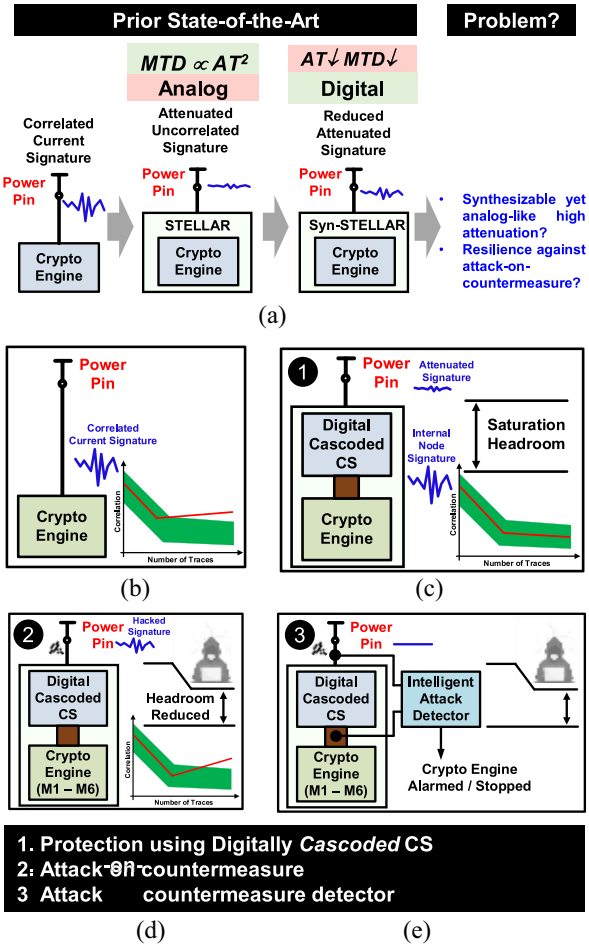


FIGURE 1. (a) Prior state-of-the-art using signature attenuation techniques. (b) Unprotected AES can be attacked using power SCA. (c) This work protects against power SCA using digitally *cascoded* CS. (d) Voltage drop-based linear-region biasing attack is explored using a signature attenuation countermeasure. (e) Implemented attack detectors can detect this attack for the resilience of signature attenuation countermeasure. Key contributions are tabulated below.

II. RELATED WORKS

This study enhances the existing state-of-the-art in single digital-friendly countermeasures by a factor of 20, achieved through utilizing a cascoded CS. Additionally, we investigate the VLB attack and its corresponding detection mechanism within the same countermeasures. Before delving into the details, we will provide a brief overview of the existing literature.

A. POWER/EM SCA COUNTERMEASURE

Power and EM SCA countermeasures can be classified into three categories: 1) architectural; 2) logic-level; and 3) physical or circuit-level. Architectural countermeasures include algorithmic shuffling [3], arithmetic countermeasure [4], and multiplicative masking [1]. Algorithmic shuffling rearranges

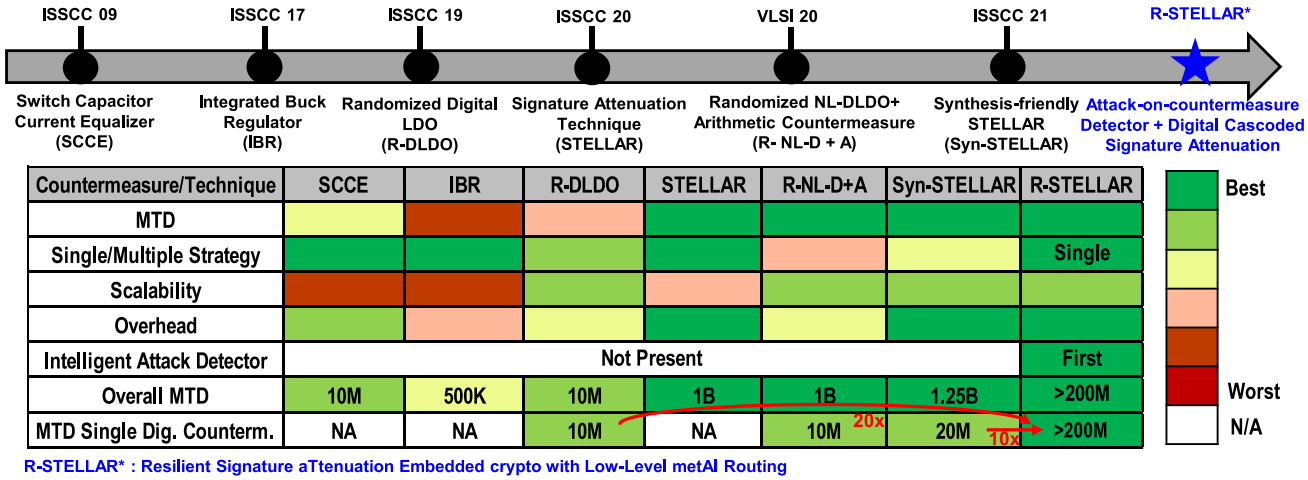


FIGURE 2. State-of-the-art circuit-level countermeasures. This work brings the benefit of cascoded CSs in the digital domain for high security, even being scalable.

cryptographic operations to disrupt the correlation between power consumption and sensitive data; however, it has limited capability against SCA as limited operations are shuffled. Time-domain signal-to-noise ratio (SNR) is still high enough to be correlated. Logic-level countermeasures mostly compensate power to gain resilience against power side-channel. WDDL [5], SABL [6], Dual Rail Precharge Logic [7], and Boolean masking [8] are examples of the logic-level countermeasures. These solutions are mostly synthesizable; however, they suffer from high power and area overhead ($>2\times$); hence, they may not be preferred within the scope of area and energy-constrained secure IoT devices. Recently explored circuit-level countermeasures [9], [10], [11], [12], [13], [14] promise lower overhead while being generic. We discuss these genres of countermeasures in detail in the next section.

B. CIRCUIT-LEVEL COUNTERMEASURES

Circuit-level countermeasures [9], [10], [11], [12], [13], [14] solve the problem of practicality as overhead is significantly less than architectural or logic-level countermeasures. This leads to a recent thrust of circuit-level/physical countermeasures against SCA. The progression of the physical countermeasures is shown in Fig. 2. One popular state-of-the-art countermeasure is switch capacitor current equalizer (SCCE) [15], [16]. SCCE reaches $> 10M$ *MTD* by supplying the AES with three parallel capacitors and bypassing the information-sensitive leakage to a dc bias. However, this solution suffers from $2\times$ performance overhead due to large droop caused in the capacitors. Voltage regulator-based solutions include integrated buck regulator (IBR [17], [18])-based solution and series LDO with loop randomization (R-DLDO [19]). They provide medium security ($<10M$ *MTD*) due to obfuscation created by different randomization techniques. However, IBR has large passives (note that MiM cap often radiates meaningful information in terms of EM emanation). Digital LDO inherently leaks critical information as voltage compensation follows the instantaneous current drawn by the crypto-engine. Digital LDO with noise injection and voltage/frequency modulation reaches 6.8M MTD against SCA, although LDO is a high-overhead solution for SCA. Cascade of NL-LDO with arithmetic countermeasures achieves ($> 1B$ *MTD*) high security against correlation power analysis (CPA). However, it suffers from high overhead due to LDO and is not generic due to arithmetic countermeasures [4], [20].

C. SIGNATURE ATTENUATION COUNTERMEASURES

STELLAR [10] achieves high MTD by using an analog cascoded CS as a power delivery circuit, which provides high attenuation due to its high output impedance. This solution achieves $> 1B$ *MTD* for the first time but is not synthesis-friendly. Syn-STELLAR [11] proposes a scalable signature attenuation-based solution that provides similar MTD ($>1.25B$ *MTD*) by cascading two solutions, namely, DSAC and time-varying transfer function (TVTF). DSAC does not provide high attenuation compared to CDSA as the synthesizable realization of CS replicates source degenerated structure instead of cascaded structure, contributing to lower attenuation. Additional ring oscillator (RO) randomization along with TVTF helped to achieve similar security (w.r.t CDSA) at the cost of high overhead. Our solution (namely, R-STELLAR) brings the benefit of analog cascoded signature attenuation in the digital domain to achieve high attenuation, hence high MTD ($> 200M$ *MTD*) against SCA. These solutions use lower metal layer routing to reduce EM leakage.

D. ATTACK AGAINST COUNTERMEASURE

Security is always a strategic contest between attackers and cryptographers. Advancements in one countermeasure may open another avenue for attack. Historically, countermeasures for square-and-multiply algorithms of RSA scheme against simple power analysis (SPA) have been attacked using differential power analysis three decades ago [21]. Another instance is when exponent randomization-based

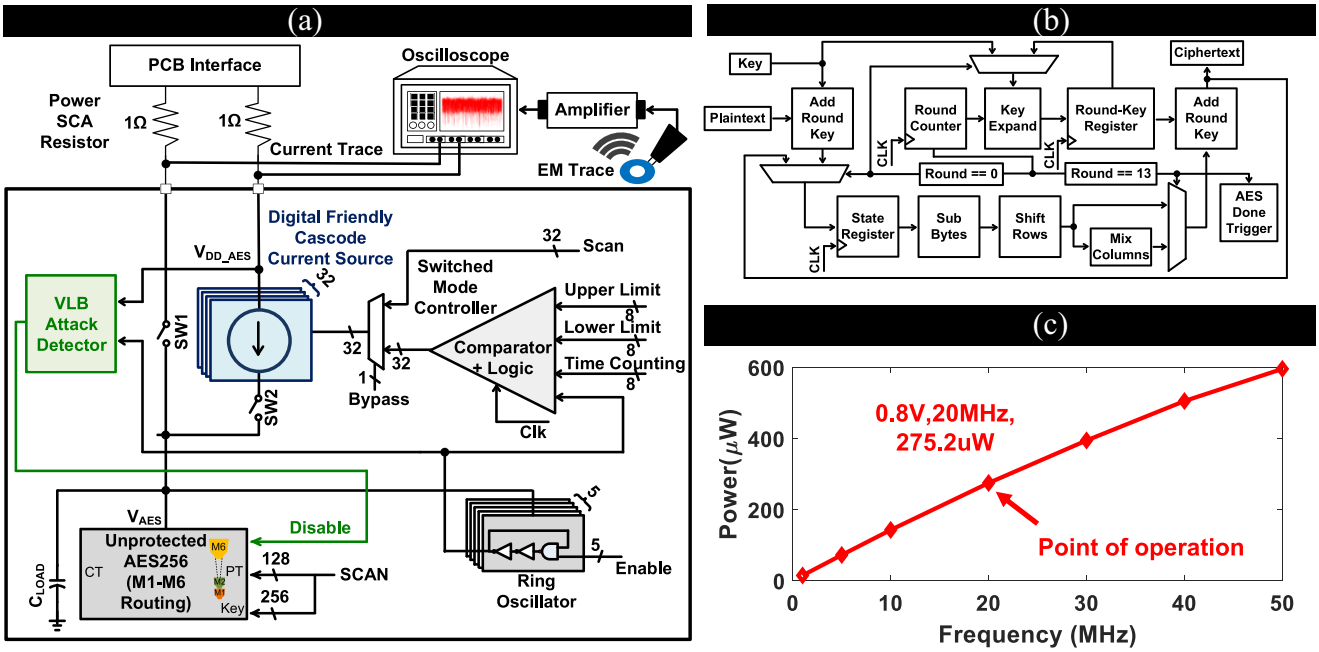


FIGURE 3. (a) Full system architecture of R-STELLAR. (b) Parallel AES-256 architecture. (c) Load characterization of AES.

countermeasures of RSA [22] have been attacked [23]. Masking is a provably secure technique. However, different masking techniques of AES have been exploited using higher order attacks or fault injection attacks (FIAs) [24]. These attack–defense–attack-based explorations of different countermeasure strategies are often explored in the standard crypto community. The recent gamut of physical countermeasures should be tested well against different types of attack strategies. As these countermeasures frequently come from circuit knowledge, attackers with knowledge of the circuit can increase the probability of attack. Hence, it is impossible to popularize generic and circuit-level countermeasures without detailed stress testing. Until now, no approach exists to evaluate the physical countermeasures implemented on custom ICs against new attacks to the best of our knowledge. For the first time, we have explored an attack possibility on physical/circuit-level countermeasures and suggest an attack detector circuit that can detect such an attack through experimental evaluation. This type of attack detector is necessary to sustain the generic countermeasures. We believe this approach will help us increase trust and applicability in physical countermeasures. Notably, this attack is a demonstration of a signature attenuation-based circuit but can be extended to different physical countermeasures as well, which can be explored as part of future works.

III. R-STELLAR COUNTERMEASURE DESIGN

Fig. 3(a) presents the full system architecture. The full system architecture consists of a DCCS, multiple scan-controlled parallel RO as the bleed path similar to [11]. The bleed path bypasses the delta changes in the supply current, thereby stabilizing the V_{AES} node voltage by providing local

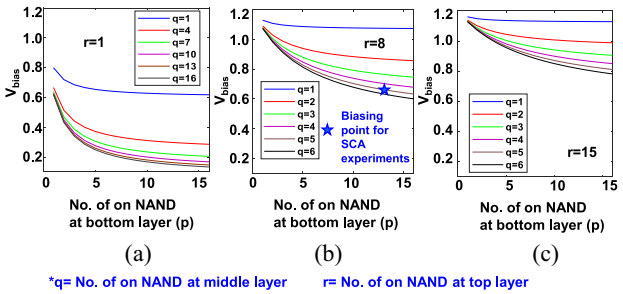


FIGURE 5. Created biasing voltage by NAND structure when the number of on NAND gate at the top *r* is (a) 1, (b) 8, and (c) 15, respectively. We create variable voltage by biasing the top pMOS of the CS slices using this structure.

negative feedback (LNFB) and hiding small key-dependent current changes. Simultaneously, the RO-bleed is the input of the global feedback (switch mode controller), which is a slow loop that compensates for process, voltage, and temperature (PVT) variation or sudden changes in the crypto current due to frequency variation of the encryption engine. We will discuss DCCS and the Global feedback loop in detail in the following subsections. Parallel AES-256 is used as an example crypto engine as shown in Fig. 3(b). Load characteristics is shown in Fig. 3(c). We will discuss AES architecture and load characteristics briefly in Section V for continuity.

A. DIGITAL CASCODED CURRENT SOURCE

The DCCS is crucial in mitigating power and EM SCA. In previous work, Das et al. [10] employed an analog cascoded CS, achieving high attenuation (and enhanced security against SCA) as shown in Fig. 4(a). However, this analog solution faces scalability challenges when transitioning to newer technology

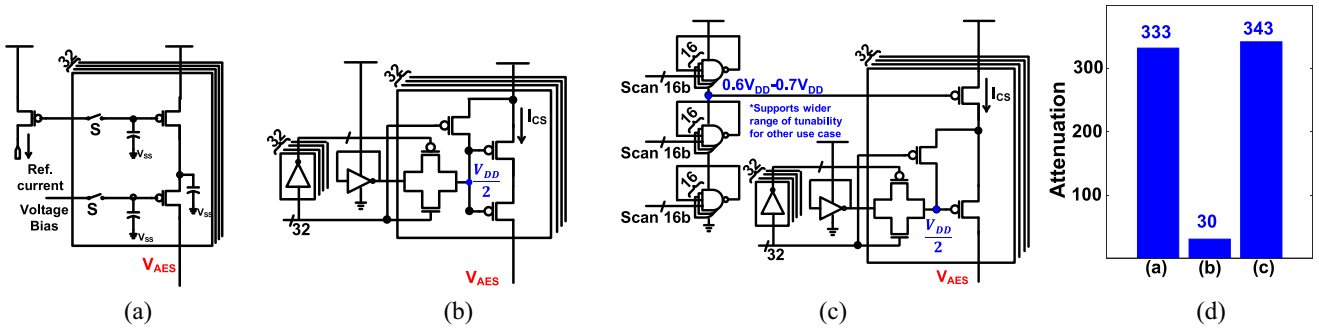


FIGURE 4. Progression of signature attenuation circuit from analog-to-digital domain: (a) analog cascoded CS, (b) digital source degenerated CS which is scalable but provides low attenuation, (c) DCCS providing very high attenuation in digital domain, and (d) attenuation by using architecture (a)–(c).

nodes. Adaptation to each technology node requires significant engineering effort. To address this, a synthesis-friendly CS was proposed by Ghosh et al. [11], as depicted in Fig. 4(b). This digital-friendly approach brings the benefits of signature attenuation in the digital domain, maintaining scalability. The work by Ghosh et al. [11] employs a pMOS-based power-gate approach for CS utilization. Specifically, a stacked pMOS structure is biased using a self-connected NOT gate, internally generating a voltage of $(V_{\text{DD}}/2)$. It is important to note that biasing NOT gate will have short-circuit current. However, minimum-sized NOT gate consumes only ∼6-uA current at $V_{\text{DD}} = 1.2$ V, making this negligible overhead with respect to the entire R-STELLAR-AES. This solution effectively addresses the scalability challenge associated with signature attenuation-based countermeasures. However, this architecture uses source-degenerated CS structures. Source degenerated CS exhibits lower output impedance than the cascoded structure, reducing attenuation. To overcome this limitation, we propose a DCCS. The DCCS configuration consists of two pMOS transistors, each independently biased, as illustrated in Fig. 4(c). The NOT gate's output is connected to its input, stabilizing it at $(V_{DD}/2)$ to bias the lower pMOS. The upper pMOS, on the other hand, is biased using a stack of NAND gates. Specifically, three stages of 16 self-connected NAND gates serve as a resistive divider. By connecting one input of the NAND gate to its output, we incorporate a self-biased structure. Importantly, the NAND gate provides control over the NOT gate. When the other input is "1," it functions as a self-biased inverter, effectively acting as a resistor in the implemented architecture. Conversely, if the other input is "0" (resulting in a NAND output "1"), the nMOS series path is closed, exhibiting high resistance (nMOS in the cut-off region). This controllability via the second input port enables a tunable resistive-divider structure, facilitating the biasing of the upper pMOS. We use these two techniques to bias the pMOS transistors, resulting in a synthesizable cascoded CS. Biasing voltage of the top pMOS (V_{bias}) is given by the following equation:

$$V_{\text{bias}} = V_{\text{DD}} \times \frac{Z_{\text{bottom}} + Z_{\text{mid}}}{Z_{\text{bottom}} + Z_{\text{mid}} + Z_{\text{top}}}$$

$$= V_{DD} \times \frac{\left(\frac{r_{\text{on}}}{p} \| \frac{r_{\text{off}}}{16-p}\right) + \left(\frac{r_{\text{on}}}{q} \| \frac{r_{\text{off}}}{16-q}\right)}{\left(\frac{r_{\text{on}}}{p} \| \frac{r_{\text{off}}}{16-p}\right) + \left(\frac{r_{\text{on}}}{q} \| \frac{r_{\text{off}}}{16-q}\right) + \left(\frac{r_{\text{on}}}{r} \| \frac{r_{\text{off}}}{16-r}\right)} \quad (1)$$

where Z_{top}, Z_{mid}, and Z_{bottom} are the impedances of different NAND stages, r_{on} and r_{off} are self-connected and off resistance of a single NAND gate, and p, q, r are the number of self-connected NAND at bottom, middle, and top stage, respectively. We can control the resistance by controlling p, q, r. Note that, assuming $r_{\text{off}} >> r_{\text{on}}$, this structure, ideally, can generate voltages between 0 and V_{DD}. However, the contribution of r_{off} restricts the full swing. For example, with 16 stages of minimum-sized NAND gates, we can generate voltage ranging from 110 mV to 1.15 V when $V_{\text{DD}} = 1.2$ V as shown in Fig. 5(a)–(c) by using p, q, r as tuning knob. We vary the number of self-connected NAND at every stage of the NAND structure and plot created biasing voltage with different numbers of top self-connected NAND gates (r). For this work, we use $V_{\text{bias}} = 0.72$ V. This approach maintains scalability while providing substantial attenuation by creating cascoded structure, positioning it as a key component in signature attenuation-based countermeasures. Power gates are often placed using a standard power gate library with an automatic place-and-route script. Similarly, the NOT/NAND-based biasing circuit is generated using a script, and the netlist is directly used for place-and-route. Thus, the entire process is automated and digital-friendly, requiring no manual intervention to generate the final GDS. However, it is important to note that not all digital libraries support power gates. Standard cell libraries that include power gates will support the place-and-route of this structure. This digital structure has $\leq 0.5\%$ variation based on different process corners. We conducted simulations across all process corners to examine the variations. This structure depends on the impedance ratio of the self-connected NAND/inverters. NAND/NOT gates at every stage behave similarly in a particular process corner, hence the impedance ratio of them remains similar, keeping variation $\leq$0.5%. Monte-Carlo simulation shows ≈11% variation (Fig. 6) in biased voltage when considering 15% mismatch variations. However, precise voltage is not

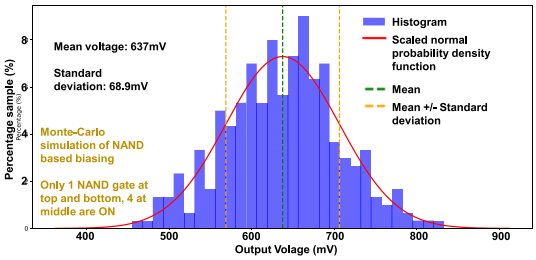


FIGURE 6. Monte-Carlo simulations. A mean voltage of 637 mV and a standard deviation of 68.9 mV are observed at the mentioned configuration.

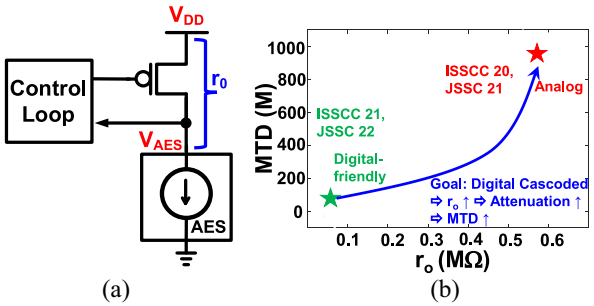


FIGURE 7. (a) LDO architecture for security. (b) Higher output impedance (r_o) helps achieving higher signature attenuation. This work achieves analog-like r_o by using the digital circuit.

A very strict requirement in this scenario. The CS should be biased in the saturation region, providing high output impedance. A feedback loop stabilizes that region in case PVT variations change the current per CS slices. The short-circuit current of this structure is very low as both the pMOS and nMOS have very low overdrive voltage (V_{GS}-V_T). This circuit is inspired by the self-biased resistive-feedback low-noise amplifier architecture, which is widely used in RF analog ICs [25]. This architecture is prevalent due to the widespread use of self-biased circuits in different contexts. Moreover, we have a set of biasing NOT/NAND gates that can be activated rotationally to mitigate the effects of aging. Notably, through parametric extracted simulations, we achieve an impressive 343× attenuation, surpassing the results reported in Ghosh et al.'s previous work (which achieved 30× attenuation [11]) as shown in Fig. 4(d). This architecture is an LDO architecture [Fig. 7(a)] which is proven effective against SCA. Note that the control loop at shunt LDO also uses a shunt path for stable internal voltage, hence providing higher security. Digital cascoded architecture helps us achieve similar high output impedance of analog structure [Fig. 7(b)]. We will explore MTD improvement through silicon experimentation, which is described in Section V.

B. SWITCHED MODE CONTROLLER AS GLOBAL FEEDBACK LOOP AND RING OSCILLATOR AS LOCAL NEGATIVE FEEDBACK

Our design uses a digital switched-mode controller (SMC) loop as global negative feedback. The adoption of SMC is prevalent in signature attenuation-based solutions, as discussed in [11]. However, an in-depth understanding of this component is crucial for assessing the attack surface against such countermeasures.

The RO converts V_{AES} voltage into frequency. RO output undergoes frequency division before being counted by an asynchronous counter. This frequency division ensures low-power operation without sacrificing precision in the asynchronous counter. A decision circuit is also employed to selectively activate or deactivate the CS slices. This dynamic adjustment responds to variations in average current drawn by the cryptographic engine due to PVT fluctuations or changes in operating frequency. While the RO is an LNFB path, it is not utilized for random noise injection, as demonstrated in Ghosh et al.'s work [11]. Our evaluation focuses purely on the signature attenuation technique for a fair comparison of the key technique. The RO also plays a role in detecting malicious voltage drop-based attacks.

IV. VOLTAGE-DROP LINEAR-REGION BIASING ATTACK

A. POSSIBILITY OF ATTACK BY MANIPULATING GNFB

The attack modality is explained in Fig. 8, involving manipulating the SMC loop. Consider an encryption engine that draws a current of $15I$, which is supplied by 15 CS slices operating in the saturation region. Now, through trial and error, an attacker can deliberately reduce the supply voltage (V_{DD}) slightly. Due to this abrupt voltage drop, the encryption engine may initially fail to operate. Still, the GNFB will engage, aiding the circuit into a steady state. To compensate for the reduced average current, the SMC loop activates additional CS slices. For instance, if each CS slice can provide $(3/4) \times I$ current, then 20 CS slices would collectively deliver the required $15I$ current for the encryption engine as shown in Fig. 8. Notably, all these slices operate in the linear region, resulting in significantly lower output impedance. Unfortunately, this reduced attenuation leads to heightened information leakage. The simulated impact of a voltage drop-based attack on the global negative feedback loop is depicted in Fig. 9. In the absence of any voltage drop, when the CS slices operate in the saturation region, there is no vulnerability to attack. The system remains stable, as shown in the red region. As the voltage (V_{DD} node) experiences a slight drop, the SMC loop becomes destabilized. Notably, a significant droop occurs at the V_{AES} node (indicated by the blue region in Fig. 9). However, an attack is not feasible in this scenario because the CS cannot supply the required current to the AES. Consequently, the AES remains nonoperational while the SMC becomes active. Eventually, the loop settles back into stability (green region). The CS slices operate in the linear region at this point, creating a lack of high attenuation. Unfortunately, this lack of high attenuation introduces the possibility of an attack. It is important to note that an attack on this countermeasure is not always possible. We need to

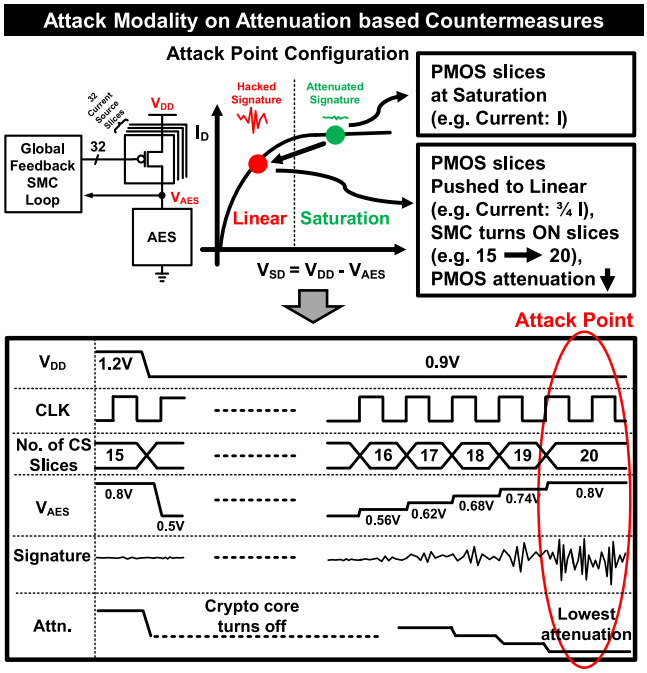


FIGURE 8. Attack modality on attenuation-based countermeasure. Manipulating the CS and operating them in the linear region while supplying enough average current for the crypto engine leads to information leakage.

meet the following circuit criterion to achieve the attack point:

$$
\begin{aligned}
I_{\text{crypto}} &= I_{\text{sat}} \times m = I_{\text{lin}} \times n \\
&\Rightarrow \frac{K}{2}(V_{GS} - V_T)^2 \times m = K(V_{GS} - V_T - V_{DS}/2)V_{DS} \times n \\
&\Rightarrow \frac{(V_{GS} - V_T)^2}{2(V_{GS} - V_T - V_{DS}/2) \times V_{DS}} \times \frac{I_{\text{Crypo}}}{I_{\text{sat}}} = n \\
&\Rightarrow n = \frac{I_{\text{crypto}}}{2K} \times \frac{1}{(V_{GS} - V_T - V_{DS/2})/V_{DS}} \\
&= \frac{1}{2K} \cdot \frac{I_{\text{Crypto}}}{\left(V_{GS} - V_T - \frac{V_{DS}}{2}\right) \times V_{DS}} \leq n_{\max} \qquad (2)
\end{aligned}
$$

where m and n are pMOS turned on to supply the crypto engine in saturation and linear region respectively; K MOS device constant, I_{crypto} is average crypto current. V_{GS}, V_{DS}, and V_T are absolute gate-to-source, drain-to-source, and threshold voltage, respectively. I_{sat} and I_{lin} are saturation and linear region current of single pMOS gates. n_{max} is maximum CS slices. Note that if all the CSs combined cannot drive the crypto core, the attack will not be successful.

Moreover, lowering the V_{DD} may stabilize AES at lower V_{AES} reducing the efficiency. This reduction can lead to setup time violations, thereby increasing the possibility to FIA. Although this specific attack is beyond the scope of this article, it is crucial to note that our attack detection technique is capable of identifying any voltage drops, thereby mitigating such risks at the source.

B. VLB ATTACK DETECTOR

We introduce an attack detection circuit to mitigate malicious VLB attacks on signature attenuation countermeasures. The

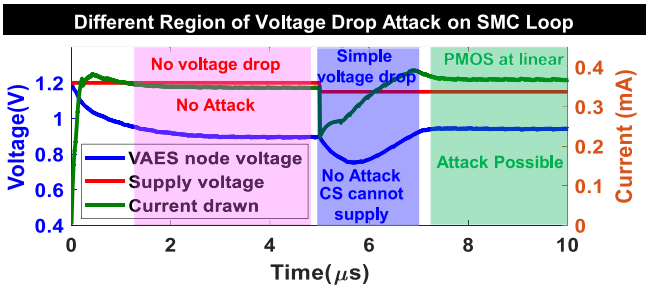


FIGURE 9. Different region for voltage drop-based attack. At stable V_{DD}, there is no voltage drop leading to no attack. Initial voltage drop cannot support this attack as CS cannot supply the AES. However, GNFB stabilizes CS slices in linear regions; it will start leaking information.

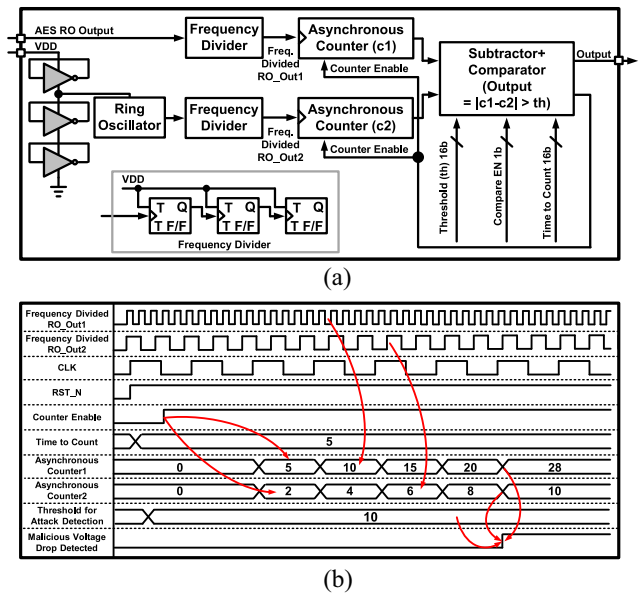


FIGURE 10. (a) Attack detector circuit for malicious VLB attack. (b) Sample waveform of attack detector.

circuit, depicted in Fig. 10(a), aims to identify the voltage discrepancy between V_{DD} and V_{AES}, enabling successful detection of malicious attacks.

Within our system, the LNFB employs an RO to stabilize the V_{AES} node, serving as an input to the GNFB. We utilize the same RO as a critical component to ensure the sustainability of our signature attenuation-based countermeasure. The RO output undergoes frequency division and feeds into an asynchronous counter, yielding an estimation of the AES voltage. Additionally, we employ another RO to estimate the global V_{DD}. By dividing the voltage using stacked inverters, we achieve approximately (2/3) of the global V_{DD}. This voltage division strategy ensures that both the counted numbers remain closely aligned. The divided voltage is digitized through a replica frequency divider and an asynchronous counter. Subsequently, both counted values are input to a digital comparator, which functions as the voltage drop detector. Ideally, the difference between these two numbers should be minimal, given the similarity between the voltage-divided V_{DD} and V_{AES}. This comparison

is configurable, allowing us to adjust the estimated difference using a scan chain within the voltage drop detector circuit. In the event of a voltage drop-based attack, where V_{DD} is intentionally reduced, the difference between the counter outputs surpasses a predefined threshold. This occurrence signals the possibility of VLB SCA on our signature attenuation-based countermeasures, ultimately activating protective measures, including halting the encryption engine. Note that the determination of the threshold is analogous to the methodology employed in built-in self-test (BIST) circuits, such as those found in digital LDOs. This similarity stems from the shared fundamental principles underlying both systems. The RO consumes approximately 3 μA of current, allowing the voltage divider circuit to supply the required low voltage. Additionally, the top-stage NAND structure offers tunability, enabling the injection of additional current in the event of a voltage drop. It is important to note that this article conceptually addresses the efficacy of the proposed voltage detector. The BIST circuit for tunability is beyond the scope of this work and will be explored in future research.

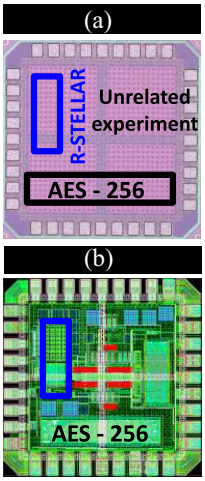
Fig. 10(b) illustrates the working principle of the attack detector. Frequency divided RO outputs (RO_Out1 deduced from V_{DD} and RO_Out2 deduced from V_{AES}) are counted using an asynchronous counter when the counter enable signal is high. "Time to count" determines the time required (# clock cycles) to accumulate RO outputs before calculating the difference between them. In this example, asynchronous counter1 and asynchronous counter2 accumulate the RO output for five clock cycles, which are 20 and 8, respectively.

The difference of 12 is greater than the expected threshold of 10, which indicates the ongoing malicious voltage drop attack. "Time to count" serves as a crucial control parameter in this context. The differences between the two counters are only measured up to the "Time to count" interval periodically. This approach prevents the accumulation of differences, thereby eliminating false positives.

V. MEASUREMENT RESULTS

A. IC SPECIFICATION

The IC micrograph is depicted in Fig. 11(a). This 1 mm^2 IC features an AES-256 crypto-engine as a use case. In particular, the left side of the IC houses the countermeasure implemented, R-STELLAR. IC layout clearly showing the important blocks is presented in Fig. 11(b). A 1-Ω resistor is used in V_{DD} series path to sense the current for power SCA. The IC specifications are summarized in Fig. 11(c). Fabricated using the TSMC 65-nm CMOS LP process, the IC employs chip-on-board packaging with glob-top encapsulation. Load characterization is performed on the unprotected core, as illustrated in Fig. 3(c). The parallel 128-bit datapath AES serves as the crypto engine [Fig. 3(b)], operating at 20 MHz and 0.8 V V_{DD}. At this configuration, AES-256 consumes 275.2 uW of power. A 30-pF decoupling capacitor (moscap) is placed, occupying an area of 0.003 mm^2. The total active area of the encryption engine is 0.14 mm^2. A



(c)

Test Chip	Process	65nm CMOS LP
	Package	Wire-bond(Glob-Top Encapsulation)
Unprotected AES-256 Core	Performance	0.8V/20MHz/275uW
	Architecture	128b Datapath (parallel AES)
	De-Cap.	30 pF MOS Cap (0.003 mm^2)
	Active Area	0.14 mm^2
	Scan Chain	387b
i-DCSAC	Input	1.2V
	Active Area	0.048 mm^2
	Decap.	30 pF MOS Cap (0.003 mm^2)
	Load Cap	150 pF MOS Cap (0.015 mm^2)
	Scan Chain	Protected core: 179b

FIGURE 11. (a) IC micrograph. (b) IC layout, blue box shows the countermeasure area. (c) IC specification.

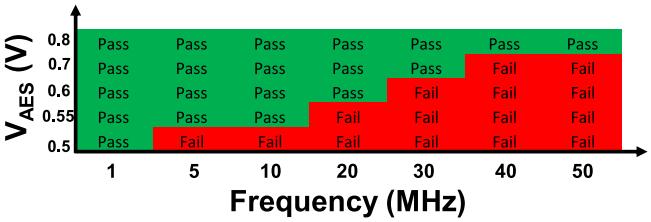


FIGURE 12. Shmoo plot: V_{AES} versus maximum frequency of AES.

Shmoo plot for V_{AES} versus maximum frequency is plotted in Fig. 12. The countermeasure occupies an active area of 0.048 mm^2. To further stabilize the V_{AES} node and provide resilience against large droops, an additional load capacitor of 150 pF is incorporated. This capacitor, occupying an area of 0.015 mm^2, contributes to area overhead significantly. R-STELLAR operates with a 1.2-V V_{DD} input. Protection needs 179 bits of scan chain for configuration, although some of these scan bits are also utilized for unrelated experiments within the same die. The proposed countermeasure is generic and can be adopted to any crypto core and operating at any frequency if CS designs are taken care of for maximum current support. For example, AES operating at higher frequency needs more average current. This requires a greater number of slices or transistors with higher W/L width.

B. MEASUREMENT SETUP

The attack setup is depicted in Fig. 13. A power trace is acquired using a 5-GSps oscilloscope, while an H-probe with a 10-mm diameter is employed for EM trace collection. The EM trace is subsequently amplified using a wideband amplifier before being acquired through the oscilloscope. The end of encryption is indicated by a trigger signal, aiding in the alignment of the collected traces. These traces are then transmitted to a computer via the VISA protocol for further processing. The computer utilizes an NI-data acquisition (NI-DAQ) card to configure the IC. Additionally, an arbitrary waveform generator (AWG) supplies the IC with enable,

TABLE 1. Comparison with respect to other state of the art.

Parameter			This Work	JSSC'23 [1]	ISSCC'21 [9]	VLSI'20 [20]	ISSCC'20 [10]	JSCC'20 [19]	ISSCC'17 [18]	ISSCC '09 [15]
Countermeasure Technique			Resilient STELLAR	Multiplicative Masking	Syn-STELLAR	NL-DLDO + Arithmetic Countermeasure	STELLAR	Digital LDO + randomization	Integrated Buck Regulator	Switched Cap. Current Equalizer
Process			65nm CMOS	7nm CMOS	65nm CMOS	14nm CMOS	65nm CMOS	130nm CMOS	130nm CMOS	130nm CMOS
Crypto Algorithm			AES-256	AES-256	AES-256	AES-128	AES-256	AES-128	AES-128	AES-128
Standalone AES Power/Frequency			275.2uW @ 20MHz, 0.8V	-	189uW @ 10MHz, 0.8V	-	0.8mW @ 50MHz, 0.8V	10.9mW @ 80MHz,0.84 V	10.5mW @ 40MHz	33mW @ 100MHz
Single Strategy			**Yes**	Yes	No	No	Yes	No	Yes	Yes
Design Overheads	Area		**35%**	65%	28% & 52%	8%[c]	36.7%	36.9%[b]	1%[a]	33%
	Power		50%	-	33% & 50%	10%[c]	49.8%	32%	5%[a]	20%
	Perf.		**0%**	4%	0%	0.7%	0%	10.4%	3.33%	50%
SCA Analysis	Time/Freq Domain		Time, Freq	Time	Time, Freq	Time	Time, Freq	Time, Freq	Time, Freq	Time
	MTD	CPA	**>200M**	850M	390M(~20M)* & >1.25B	1B (>1,00,000x)	>1B (1,25,000x)	8M (4210x)	>100K (20x)	>10M (2500x)
		CEMA	**>200M**	>1B	248M(~20M)* & >1.25B	1B (>1,00,000x)	>1B (>83,333x)	6.8M (136x)	-	-
		Power TVLA	**>500,000x**	35,000x	195,000x & 290,000x	>250,000x	-	-	-	-
		EM TVLA	**>250,000x**	>38,000x	>50,000x &>70,000x	>250,000x	-	-	-	-
	Attack Mode		Power/EM	Power/EM	Power/EM	Power/EM	Power/EM	Power/EM	Power	Power
	Attack on Countermeasure Detection		**Yes**	-	-	-	-	-	-	-

[a]Regulator area/power not included, [b]Cap area not included, [c]DLDO area/power not included. Area overhead >150% with DLDO (estimated), *20M MTD without bleed randomization (with only digital CS).

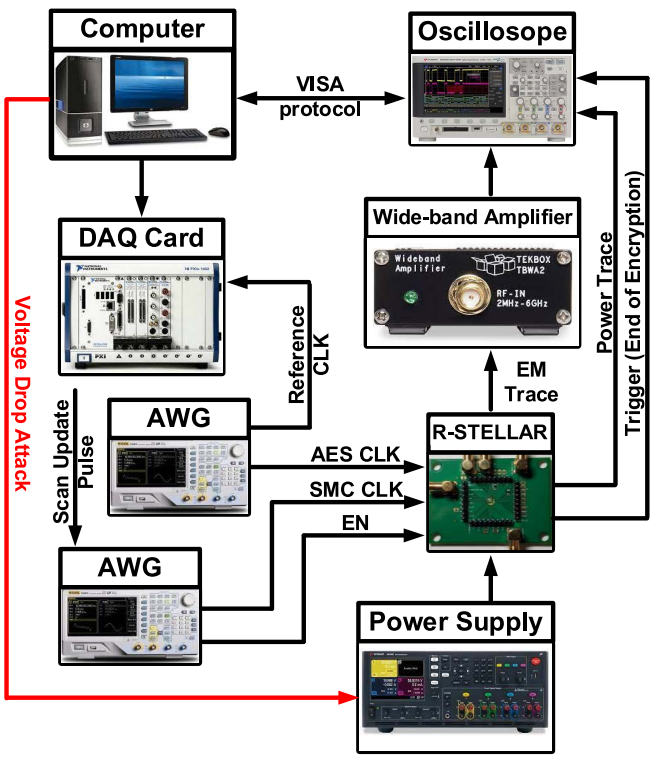


FIGURE 13. Measurement setup for power/EM side channel.

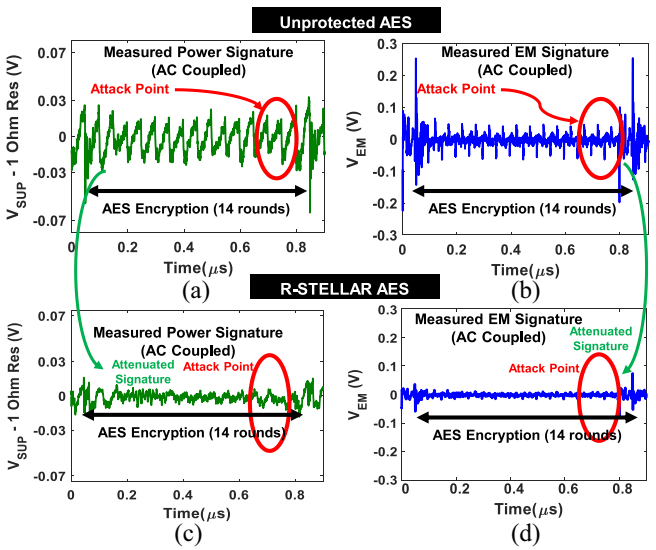


FIGURE 14. Time-domain trace for different configurations: (a) unprotected power, (b) unprotected EM, (c) protected power, and (d) protected EM.

reset, and clock signals. Typically, a stable power supply powers up the IC. But here, we control the supply from the computer to introduce a VLB attack. All the experiments are done in room temperature (~25 °C).

C. CORRELATIONAL POWER/EM ATTACK AND LEAKAGE ANALYSIS

The time-domain measurement results are depicted in Fig. 14. In Fig. 14(a), the ac-coupled power trace is displayed, showing 14 cycles of AES operation. Fig. 14(b) presents the amplified ac-coupled EM trace. Additionally, Fig. 14(c) shows the attenuated power trace. Finally, Fig. 14(d) displays the attenuated EM traces. Attenuation is clearly visible when CS is operating in the saturation region. We have chosen the HD between the last two rounds as our

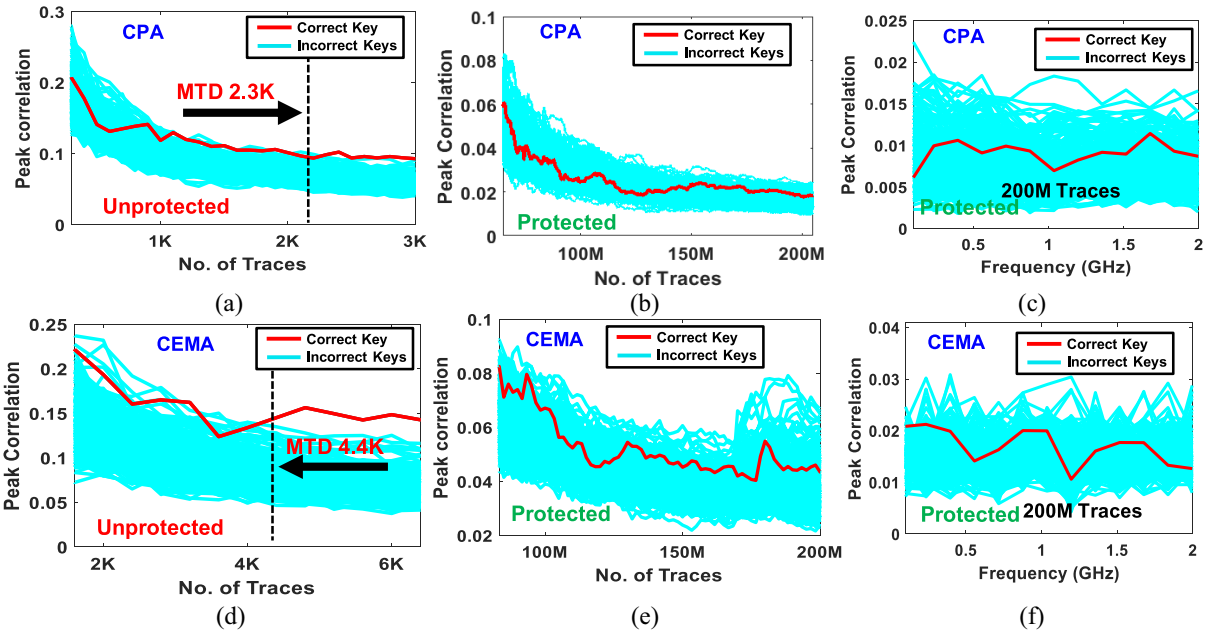


FIGURE 15. CPA on (a) unprotected AES-256, (b) protected AES-256, and (c) frequency-domain CPA on protected AES-256. CEMA on (d) unprotected AES-256, (e) protected AES-256, and (f) frequency-domain CEMA on protected AES-256.

attack model. The correct key is revealed within 2.3K traces in the standard correlational power attack, as depicted in Fig. 15(a) for the unprotected implementation. However, in the presence of R-STELLAR, the correct key is not revealed even after analyzing 200M traces [Fig. 15(b)]. To further validate our findings, we conducted a frequency-domain CPA over a frequency range of 1 MHz to 2 GHz [Fig. 15(c)]. No peak correlation is detected across the entire spectrum. It is worth noting that attackers often attempt to mitigate the effects of noise by averaging traces, thereby increasing the SNR. Our attack setup follows a similar approach, employing an averaging factor of 1000 during the attack. In contrast, standard correlation EM analysis (CEMA) with the HD between the last two rounds successfully reveals the correct key using just 4.4K traces [Fig. 15(d)]. No correct key byte is exposed even after analyzing 200M traces using CEMA [Fig. 15(e)]. We performed frequency-domain CEMA on a protected AES implementation to ensure security in the frequency domain. No key byte is revealed when measured with 200M traces across the entire frequency spectrum of 1 MHz to 2 GHz [Fig. 15(f)].

TVLA-based leakage analysis was conducted on both unprotected and protected implementations. The $|t| - value$ was calculated using fixed and random plaintexts. A $|t| - value$ exceeding 4.5 indicates the presence of a leaky component. The unprotected implementation starts to leak within 100 traces for both the power and EM side channels. The countermeasure, R-STELLAR, shows the presence of leakage after 2.5M and 5M traces for EM and power SCA, respectively, as shown in Fig. 16. This is 250 000× and 500 000× improvement with respect to unprotected implementation.

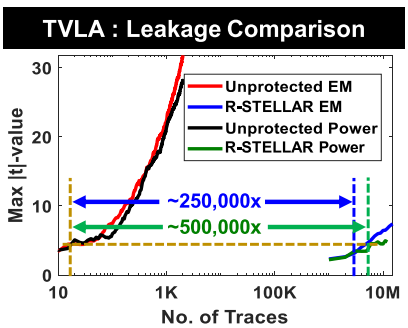


FIGURE 16. TVLA-based leakage analysis for all configurations.

D. MALICIOUS VOLTAGE DROP-BASED ATTACK AND MITIGATION

For the first time, we explore a dedicated SCA on a physical countermeasure. Our approach leverages a malicious voltage drop-based attack, which reduces the attenuation that the implemented power delivery circuit provides. Specifically, the pMOS begins to operate in the linear region due to a slight voltage drop at V_{DD} node. Fig. 17 presents the measured time-domain trace. Notably, the amplitude of the power trace significantly increases compared to steady-state operation [Fig. 17(b) versus Fig. 17(a)]. Following the malicious voltage drop, we incorporate a CPA. The correct key byte is retrieved with just 105K traces [Fig. 18(a)]. We perform a frequency-domain CPA using 150K traces to validate our findings further. The results confirm the presence of leaky components at 400 MHz. Additionally, we conduct a TVLA-based leakage analysis, revealing that meaningful information leakage begins from just 3K traces [Fig. 18(b)].

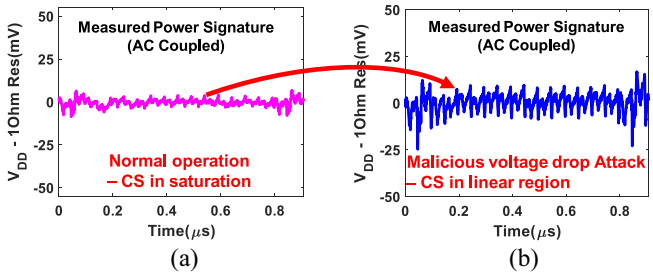


FIGURE 17. AC-coupled power trace is observed for (a) protected AES-256 and (b) protected AES-256 under malicious voltage drop-based attack.

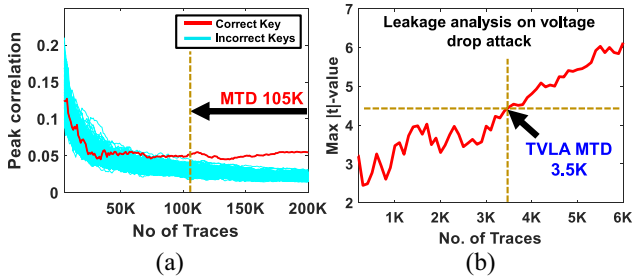


FIGURE 18. (a) MTD is reduced to 105K by malicious vVLB attack. (b) TVLA MTD (traces required to reach max $|t|$ – *value* of 4.5) reduces to 3.5K.

The proposed mitigation technique effectively detects the described attack within a time frame of 0.8 ms, achieving 100% accuracy, as illustrated in Fig. 19. Notably, the short detection time ensures the countermeasure's robustness. Assuming reduced MTD of 105K, AES operating at 20 MHz, and 14 cycles of operations, an SCA attack can be successful within 73.5 ms assuming 0 oscilloscope capture time. Notably, 0 oscilloscope capture time is unrealistic. Nevertheless, our approach detects an attack-on-countermeasure within 0.8 ms. Only 1.1% of the encryptions are possible in this time frame, eliminating the possibility of attack. The latency for attack detection is also influenced by the clock period of the attack detector. While we typically operate at a low frequency (10 kHz) due to the slow nature of the SMC loop, a faster clock could further enhance the detection speed if needed in future scenarios. Table 1 provides a comparative analysis between our proposed work and existing state-of-the-art techniques. It is important to note that the scan chain is typically used to configure the circuit once at the beginning of the testing. Even in the absence of a countermeasure, the IC would still need to be configured. Therefore, the performance overhead is considered negligible.

VI. CONCLUSION

Our approach offers a scalable physical countermeasure while maintaining high security as a standalone technique. Importantly, no attacks have been explored on these countermeasures to date. In this work, we investigate an attack on the countermeasure circuit for the first time and introduce a detector circuit to identify such attacks. In summary, our work achieves over 200M MTD with synthesizable

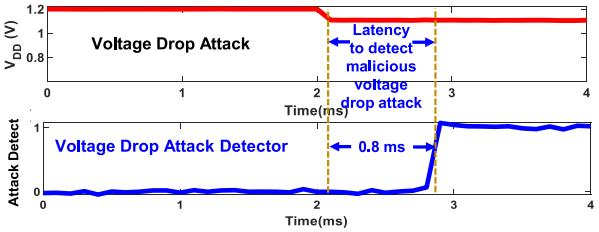


FIGURE 19. Attack detector can detect such attack within 0.8 ms.

signature attenuation as a single countermeasure technique. Additionally, we explore an attack modality in the presence of physical countermeasures, specifically focusing on synthesizable signature attenuation. Our proposed method effectively detects supply voltage drop-based linear-region biasing attacks within less than 1 ms. Practical CPA within this time range is infeasible. Furthermore, this generic countermeasure can be cascaded with other algorithmic or architectural countermeasures to enhance overall security.

REFERENCES

[1] R. Kumar et al., "A 7-Gbps SCA-resistant multiplicative-masked AES engine in Intel 4 CMOS," *IEEE J. Solid-State Circuits*, vol. 58, no. 4, pp. 1106–1116, Apr. 2023.

[2] *TEMPEST Attacks Against AES*, Fox-IT, Fuzhou, China, Accessed: Sep. 5, 2020.

[3] B. Yu, X. Li, C. Chen, Y. Sun, L. Wu, and X. Zhang, "An AES chip with DPA resistance using hardware-based random order execution," *J. Semicond.*, vol. 33, no. 6, Jun. 2012, Art. no. 65009.

[4] R. Kumar et al., "A SCA-resistant AES engine in 14nm CMOS with time/frequency-domain leakage suppression using non-linear digital LDO cascaded with arithmetic countermeasures," in *Proc. IEEE Symp. VLSI Circuits*, 2020, pp. 1–2.

[5] D. D. Hwang et al., "AES-based security coprocessor IC in 0.18-um CMOS with resistance to differential power analysis side-channel attacks," *IEEE J. Solid-State Circuits*, vol. 41, no. 4, pp. 781–792, Apr. 2006.

[6] M. Bucci, L. Giancane, R. Luzzi, and A. Trifiletti, "Three-phase dual-rail pre-charge logic," in *Proc. 8th Int. Workshop Cryptogr. Hardw. Embed. Syst.*, 2006, pp. 232–241.

[7] 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 Eur. Solid-State Circuits Conf.*, 2002, pp. 403–406.

[8] A. Poschmann, A. Moradi, K. Khoo, C.-W. Lim, H. Wang, and S. Ling, "Side-channel resistant crypto for less than 2,300 GE," *J. Cryptol.*, vol. 24, no. 2, pp. 322–345, Apr. 2011.

[9] 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 *Proc. IEEE Int. Solid-State Circuits Conf. (ISSCC)*, 2021, pp. 499–501.

[10] D. Das et al., "27.3 EM and power SCA-resilient AES-256 in 65nm CMOS through >350× current-domain signature attenuation," in *Proc. IEEE Int. Solid-State Circuits Conf. (ISSCC)*, 2020, pp. 424–426.

[11] A. Ghosh, D. Das, J. Danial, V. De, S. Ghosh, and S. Sen, "Syn-STELLAR: An EM/power SCA-resilient AES-256 with synthesis-friendly signature attenuation," *IEEE J. Solid-State Circuits*, vol. 57, no. 1, pp. 167–181, Jan. 2022.

[12] Y. He and K. Yang, "25.3 a 65nm edge-chasing quantizer-based digital LDO featuring 4.58ps-FoM and side-channel-attack resistance," in *Proc. IEEE Int. Solid-State Circuits Conf. (ISSCC)*, 2020, pp. 384–386.

[13] A. Ghosh, D.-H. Seo, D. Das, S. Ghosh, and S. Sen, "A digital cascoded signature attenuation countermeasure with intelligent malicious voltage drop attack detector for em/power SCA resilient parallel AES-256," in *Proc. IEEE Custom Integr. Circuits Conf. (CICC)*, 2022, pp. 1–2.
[14] A. Ghosh, M. A. Rahman, D. Das, S. Ghosh, and S. Sen, "Power and EM SCA resilience in 65nm AES-256 exploiting clock-slew dependent variability in CMOS digital circuits," in *Proc. IEEE Custom Integr. Circuits Conf. (CICC)*, 2023, pp. 1–2.
[15] C. Tokunaga and D. Blaauw, "Secure AES engine with a local switched-capacitor current equalizer," in *IEEE Int. Solid-State Circuits Conf. Tech. Dig.*, 2009, pp. 64–65.
[16] C. Tokunaga and D. Blaauw, "Securing encryption systems with a switched capacitor current equalizer," *IEEE J. Solid-State Circuits*, vol. 45, no. 1, pp. 23–31, Jan. 2010.
[17] M. Kar, A. Singh, S. Mathew, A. Rajan, V. De, and S. Mukhopadhyay, "8.1 improved power-side-channel-attack resistance of an AES-128 core via a security-aware integrated buck voltage regulator," in *Proc. IEEE Int. Solid-State Circuits Conf. (ISSCC)*, 2017, pp. 142–143.
[18] M. Kar, A. Singh, S. K. Mathew, A. Rajan, V. De, and S. Mukhopadhyay, "Reducing power side-channel information leakage of AES engines using fully integrated inductive voltage regulator," *IEEE J. Solid-State Circuits*, vol. 53, no. 8, pp. 2399–2414, Aug. 2018.
[19] A. Singh et al., "Enhanced power and electromagnetic SCA resistance of encryption engines via a security-aware integrated all-digital LDO," *IEEE J. Solid-State Circuits*, vol. 55, no. 2, pp. 478–493, Feb. 2020.
[20] R. Kumar et al., "A time-/frequency-domain side-channel attack resistant AES-128 and RSA-4K crypto-processor in 14-nm CMOS," *IEEE J. Solid-State Circuits*, vol. 56, no. 4, pp. 1141–1151, Apr. 2021.
[21] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proc. 19th Annu. Int. Cryptol. Conf. Adv. Cryptol. (CRYPTO)*, 1999, pp. 388–397.
[22] J.-S. Coron, "Resistance against differential power analysis for elliptic curve cryptosystems," in *Proc. 1st Int. Workshop Cryptogr. Hardw. Embed. Syst. (CHES)*, 1999, pp. 292–302.
[23] P.-A. Fouque, D. Réal, F. Valette, and M. Drissi, "The carry leakage on the randomized exponent countermeasure," in *Proc. 10th Int. Workshop Cryptogr. Hardw. Embed. Syst.*, 2008, pp. 198–213.
[24] S. Saha, P. Ravi, D. Jap, and S. Bhasin, "Non-profiled side-channel assisted fault attack: A case study on DOMREP," in *Proc. Design, Autom. Test Europe Conf. Exhib. (DATE)*, 2023, pp. 1–6.
[25] F. Bruccoleri, E. A. M. Klumperink, and B. Nauta, "Wide-band CMOS low-noise amplifier exploiting thermal noise canceling," *IEEE J. Solid-State Circuits*, vol. 39, no. 2, pp. 275–282, Feb. 2004.

ARCHISMAN GHOSH (Graduate Student Member, IEEE) received the B.E. degree in electronics and telecommunication engineering from Jadavpur University, Kolkata, India, in 2017, and the Ph.D. degree from Purdue University, West Lafayette, IN, USA, in 2024.

He is currently a Digital IC Design Lead with Ixana, West Lafayette. Prior to his Ph.D., he worked with Samsung Semiconductor India Research and Development, Bengaluru, India, for two years. He has interned with Intel Labs, Hillsboro, OR, USA. His research interests include digital SoC design and hardware security.

Dr. Ghosh was a recipient of the prestigious ECE Meissner Fellowship from Purdue University as an incoming graduate student from 2019 to 2020 and the Bilsland Dissertation Fellowship at Purdue University for his exceptional contributions as a graduate student. He was one of the recipients of the prestigious IEEE SSCS Pre-Doctoral Achievement Award in 2022.

DONG-HYUN SEO received the B.S. degree in electronics and radio engineering from Kyung Hee University, Seoul, South Korea, in 2013, the M.S. degree in electronics and computer engineering from Hanyang University, Seoul, in 2015, and the Ph.D. degree in electrical engineering from Purdue University, West Lafayette, IN, USA, in 2023.

He worked as a Senior RFIC Design Engineer with Qualcomm, Santa Clara, CA, USA, in 2023, and a Staff Analog Circuit Design Engineer with SKHynix America, San Jose, CA, USA, in 2024. He is currently working as a Component Design Engineer with Solidigm, Rancho Cordova, CA, USA. His research interests lie in the area of analog and mixed-signal circuits and systems for the NAND flash memory applications.

DEBAYAN DAS (Member, IEEE) received the Bachelor of Electronics and Telecommunication Engineering degree from Jadavpur University, Kolkata, India, in 2015, and the M.S. and Ph.D. degrees in electrical and computer engineering from Purdue University, West Lafayette, IN, USA, in 2021.

He is an Assistant Professor with the Department of Electronic Systems Engineering, Indian Institute of Science (IISc), Bengaluru, India. He worked as a Security Researcher with Intel, Hillsboro, OR, USA, from 2021 to 2022 and a Research Scientist with Intel Labs, Hillsboro, from 2022 to 2023. Before his Ph.D., he worked as an Analog Design Engineer at a startup based in India. He has interned with the Security Research Lab, Intel Labs in Summer 2018 and Summer 2020. He has authored/co-authored more than 65 peer-reviewed conferences and journals, including two book chapters and three U.S. patents. His research interests include mixed-signal IC design, biomedical circuits, and hardware security.

Dr. Das was awarded the Pratiksha Young Investigator by IISc from 2023 to 2024. He received the IEEE HOST Best Student Paper Award in 2017 and 2019, the IEEE CICC Best Student Paper Award in 2021, the Third Best Poster Award in IEEE HOST 2018, and the 2nd Best Demo Award in HOST 2020. In 2019, one of his papers was recognized as a Top Pick in Hardware and Embedded Security. He was recognized as the winner (third place) of the ACM ICCAD 2020 Student Research Competition. During his Ph.D., he was awarded the ECE Fellowship from 2016 to 2018, the Bilsland Dissertation Fellowship from 2020 to 2021, the SSCS Pre-Doctoral Achievement Award in 2021, and the Outstanding Graduate Student Research Award by the College of Engineering, Purdue University in 2021 for his outstanding overall achievements. He is currently serving as a Guest Editor for the IEEE SOLID-STATE CIRCUIT LETTERS and a Program Chair for the IEEE International Conference on Intelligent Computing and Systems at the Edge. He has been a Technical Program Committee Member, Track Chair, and primary reviewer for multiple reputed journals and conferences, including IEEE JOURNAL OF SOLID-STATE CIRCUITS, CICC, IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—PART I: REGULAR PAPERS, IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS, IEEE TRANSACTIONS ON COMPUTER-AIDED DESIGN OF INTEGRATED CIRCUITS AND SYSTEMS, ISLPED, IEEE DESIGN & TEST, *ACM Transactions on Design Automation of Electronic Systems*, IEEE JOURNAL ON EMERGING AND SELECTED TOPICS IN CIRCUITS AND SYSTEMS, IEEE TRANSACTIONS ON BIOMEDICAL ENGINEERING, IEEE ACCESS, IEEE INTERNET OF THINGS JOURNAL, DAC, GLSVLSI, IMS, and *VLSI Design*.

SANTOSH GHOSH (Member, IEEE) received the B.Tech. degree from Department of CSE, Haldia Institutes of Technology, India, in 2002, and the M.S. and Ph.D. degrees from Department of CSE, Indian Institute of Technology Kharagpur, Kharagpur, India, in 2008 and 2011, respectively.

He is a GPU Hardware Security Architect with NVIDIA, Hillsboro, OR, USA. He defines and drives cutting-edge security and cryptographic solutions for next-generation, high-performance GPU platforms—powering the world's most widely used GPUs for AI training and inference workloads. He has over 12 years of experience in architecting, optimizing, and implementing innovative security protocols across CPU, GPU, SoC, and platform-level security. His expertise spans post-quantum cryptographic (PQC) schemes, low-latency cryptography (LWC), and emerging memory safety architectures. Previously, he served as a Principal Engineer and a Security Research Leader with Intel, Hillsboro, where he led the development of multiple classical, post-quantum, and lightweight cryptographic technologies. These were applied to areas, such as secure boot, secure debug, confidential computing, and protections against physical attacks—and are now deployed across high-volume Intel CPUs. He also served as the Principal Investigator with the Intel Crypto Frontiers Research Center, focusing on PQC and LWC. He has co-authored over 80 research publications in top-tier international conferences and journals, and holds 117 U.S. patents (71 granted and 46 pending) in cryptography. In addition to industry work, he mentors academic research groups and actively contributes to the research community as a technical program committee member and reviewer for leading conferences and journals.

Dr. Ghosh's contributions were recognized with several Gordy Awards and Outstanding Employee Awards. He is currently serving on the ISSCC Security Subcommittee.

SHREYAS SEN (Senior Member, IEEE) received the bachelors degree from Jadavpur University, Kolkata, India, in 2006, and the Ph.D. degree in ECE from Georgia Tech, Atlanta, GA, USA, in 2011.

He is an Elmore Associate Professor of ECE and BME with Purdue University, West Lafayette, IN, USA. He serves as the Director of the Center for Internet of Bodies, Purdue University. He has authored/co-authored three book chapters, over 200 journal and conference paper and has 25 patents granted/pending. His current research interests span mixed-signal circuits/systems and electromagnetics for the Internet of Bodies and hardware security.

Dr. Sen is a recipient of the NSF CAREER Award in 2020, the AFOSR Young Investigator Award in 2016, the NSF CISE CRII Award in 2017, the Intel Outstanding Researcher Award in 2020, the Google Faculty Research Award in 2017, the Purdue CoE Early Career Research Award in 2021, the Intel Labs Quality Award in 2012 for industry-wide impact on USB-C type, the Intel Ph.D. Fellowship in 2010, the IEEE Microwave Fellowship in 2008, the GSRC Margarida Jacome Best Research Award in 2007, and nine best paper awards, including IEEE CICC 2019 and 2021 and IEEE HOST 2017–2020, for four consecutive years. He is the inventor of the Electro-Quasistatic Human Body Communication, or Body as a Wire technology, for which, he is the recipient of the MIT Technology Review top-10 Indian Inventor Worldwide under 35 (MIT TR35 India) Award in 2018 and Georgia Tech 40 Under 40 Award in 2022. To commercialize this invention, he founded Ixana and serves as the Chairman and the CTO and led Ixana to awards, such as the 2x CES Innovation Award in 2024, the EE Times Silicon 100, and the Indiana Startup of the Year Mira Award in 2023. His work has been covered by 250+ news releases worldwide, invited appearance on TEDx Indianapolis, NASDAQ live Trade Talks at CES 2023, Indian National Television CNBC TV18 Young Turks Program, NPR subsidiary Lakeshore Public Radio, and the CyberWire podcast. His work was chosen as one of the top-10 papers in the Hardware Security field (TopPicks 2019). He serves/has served as an Associate Editor for IEEE SOLID-STATE CIRCUITS LETTERS, *Nature Scientific Reports*, *Frontiers in Electronics*, and IEEE DESIGN & TEST, an Executive Committee Member of IEEE Central Indiana Section, and a Technical Program Committee Member of ISSCC, CICC, DAC, CCS, IMS, DATE, ISLPED, ICCAD, ITC, and VLSI Design.