# EM and Power SCA-Resilient AES-256 Through >350× Current-Domain Signature Attenuation and Local Lower Metal Routing

Debayan Das, *Member, IEEE*, Josef Danial, Anupam Golder, *Graduate Student Member, IEEE*, Nirmoy Modak, *Graduate Student Member, IEEE*, Shovan Maity, *Graduate Student Member, IEEE*, Baibhab Chatterjee, *Graduate Student Member, IEEE*, Dong-Hyun Seo, Muya Chang, *Graduate Student Member, IEEE*, Avinash L. Varna, *Member, IEEE*, Harish K. Krishnamurthy, *Senior Member, IEEE*, Sanu Mathew, *Fellow, IEEE*, Santosh Ghosh, Arijit Raychowdhury, *Senior Member, IEEE*, and Shreyas Sen, *Senior Member, IEEE*

***Abstract*— Mathematically secure cryptographic algorithms, when implemented on a physical substrate, leak critical "side-channel" information, leading to power and electromagnetic (EM) analysis attacks. Circuit-level protections involve switched capacitor, buck converter, or series low-dropout (LDO) regulator-based implementations, each of which suffers from significant power, area, or performance tradeoffs and has only achieved a minimum traces to disclosure (MTD) of $10M$ till date. Utilizing an in-depth white-box model, this work, for the first time, focuses on signature suppression in the current domain, which provides an $Attenuation^2$ enhancement in MTD, leading to orders of magnitude improvement in both power and EM side-channel analysis (SCA) immunities. Using a combination of current-domain "signature attenuation" (CDSA) along with local lower level metal routing, the critical correlated information in the crypto current is significantly suppressed before it reaches the supply pin. Especially, to prevent the EM leakage from its source (metal layers carrying the correlated crypto current acting as antennas), this work embraces lower level metal routing of the CDSA embedding the crypto-IP so that the signature becomes highly suppressed before it passes through the higher metal layers (which radiates significantly) to connect to the external pin. The 65-nm CMOS test chip contains both protected and unprotected parallel AES-256 implementations, running at a clock frequency of 50 MHz. Test vector leakage assessment (TVLA) on the protected CDSA-AES, demonstrated with on-chip measurements for the first time, shows that the higher level metal layers leak significantly more compared with the lower level metal routing. Correlational power and EM analysis (CPA/CEMA) attacks on the unprotected implementation were able to extract the secret key within $8k$ and $12k$ traces, respectively, while the protected CDSA-AES could not be broken even after $1B$ encryptions for both power and EM SCA, evaluated both in the time and frequency domains, showing an improvement of 100× over the prior state-of-the-art countermeasures with comparable power and area overheads.**

***Index Terms*— AES-256, correlational power analysis, current-domain signature attenuation (CDSA), electromagnetic (EM) leakage, hardware security, lower level metal routing, side-channel attacks, white-box analysis.**

Manuscript received May 5, 2020; revised August 3, 2020; accepted October 9, 2020. Date of publication November 24, 2020; date of current version December 24, 2020. This article was approved by Guest Editor Dejan Markovic. This work was supported in part by the National Science Foundation (NSF) under Grant CNS 17-19235 and Grant CNS 19-35573, and in part by Intel Corporation. *(Corresponding author: Debayan Das.)*

Debayan Das, Josef Danial, Nirmoy Modak, Shovan Maity, Baibhab Chatterjee, Dong-Hyun Seo, and Shreyas Sen are with the School of Electrical and Computer Engineering, Purdue University, West Lafayette, IN 47907 USA (e-mail: das60@purdue.edu; shreyas@purdue.edu).

Anupam Golder, Muya Chang, and Arijit Raychowdhury are with the School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA 30332 USA.

Avinash L. Varna is with Intel Corporation, Chandler, AZ 85226 USA.

Harish K. Krishnamurthy, Sanu Mathew, and Santosh Ghosh are with Intel Labs, Hillsboro, OR 97124 USA.

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

Digital Object Identifier 10.1109/JSSC.2020.3032975

## I. Introduction

THE huge gamut of today's Internet-connected embedded devices has led to increasing concerns regarding the security and confidentiality of data. To address these requirements, most embedded devices employ cryptographic algorithms that are computationally secure. Despite such mathematical guarantees, as these algorithms are implemented on a physical platform, they leak critical information in the form of power consumption [1], electromagnetic (EM) radiation [2], timing [3], cache hits and misses, and so on, leading to side-channel analysis (SCA) attacks. Power/EM SCA attacks can be broadly classified into non-profiled and profiled [4], [5] attacks, which involves a training phase and an attack phase. This work focuses on non-profiled SCA attacks, such as differential/correlational power/EM analysis (DPA/CPA/DEMA/CEMA), which are direct attacks on a single device to extract the secret key of an encryption algorithm [6].

### A. Motivation

Recently, AES-256 was shown to be broken in 5 min from a 1-m distance (and within few seconds from 30 cm away) using noninvasive EM probes [7]. The time-complexity of breaking an AES-256 is reduced from $2^{256}$ for brute-force attacks to $2^{13}$ for SCA attacks. Transitioning from AES-128 to

AES-256 increases the mathematical security exponentially; however, the SCA security only increases linearly by 2×.

For performing an EM/power SCA attack, first, the EM/power traces are measured from the crypto engine using an oscilloscope or a high-resolution analog-to-digital converter (ADC). Next, a hamming weight (HW) or a hamming distance (HD) model is built for different key guesses depending on the point of attack. Finally, correlation is performed between the collected traces ($T$) and the attack model ($H$), and the correct key showing the highest correlation emerges out after multiple traces are analyzed. These correlational attacks (CEMA/CPA) do not require any prior timing information on the occurrence of the targeted operation since the correlation coefficient $\rho_{TH}$ can be calculated at each time sample of the EM/power trace [8].

A HW-based attack is often effective for software crypto implementations running on a microcontroller, while HD attacks are more prominent on efficient hardware implementations as operations are more parallelized. Also, the point of attack on a crypto algorithm may change from software to hardware implementations. For instance, in the case of software AES-256, the output of the first round S-box can be targeted to derive the key using the chosen plaintexts (PTs). However, for hardware implementations, attacking combinational logic is not easy (due to the different delays for different inputs). Hence, in the case of a hardware AES-256 parallel datapath implementation, a known ciphertext (CT)-based attack on the HD for the last two rounds (13th and 14th) is more effective and practical and has been adopted for this work to evaluate the resiliency of both the unprotected and protected versions of the AES-256.

Real-world examples of EM/power SCA attacks include counterfeiting e-cigarette batteries by stealing the fixed secret key embedded in the authentic device to gain market share. Also, recently, SCA attacks on bitcoin wallets were demonstrated to recover the private key. In general, these attacks can be used to obtain the secret key from the boot-loader of any embedded device [9].

As the attacks are constantly improving and attackers are becoming even more powerful with the advent of better EM probes, it is imperative that we devise energy-efficient generic techniques to protect against both EM/power SCA attacks for any crypto algorithm. Circuit-level on-chip countermeasures include switched capacitor current equalizer [10], charge recovery logic [11], IVR [12], and all-digital low dropout (LDO) [13], which suffers from performance degradation, high power, and area overheads because of large embedded passives, as well as EM leakage from large MIM capacitor top plates.

### *B. Key Concepts*

In this work, aided by the white-box analysis of the EM leakage from a crypto-IC, we strive to tackle the problem of EM leakage at its source [14]. Fig. 1(a) and (b) shows the overview of the proposed current-domain signature attenuation (CDSA) countermeasure, which provides a significant signature suppression such that the MTD is improved by a factor of $Attenuation^2$ ($AT^2$) [15]. It should be noted that, in the security/side-channel community, the signal-to-noise ratio (SNR) is defined as the ratio of the variances of the power/EM trace and the noise, while, in our work, SNR is considered as the ratio of the voltages, as defined within the circuits community [see Fig. 1(a)]. The lower level metal routing of the CDSA embedding the crypto core ensures that only the suppressed critical signature passes through the higher metal layers, thereby simultaneously protecting against both power and the EM SCA attacks. This will be discussed in detail in Section III.

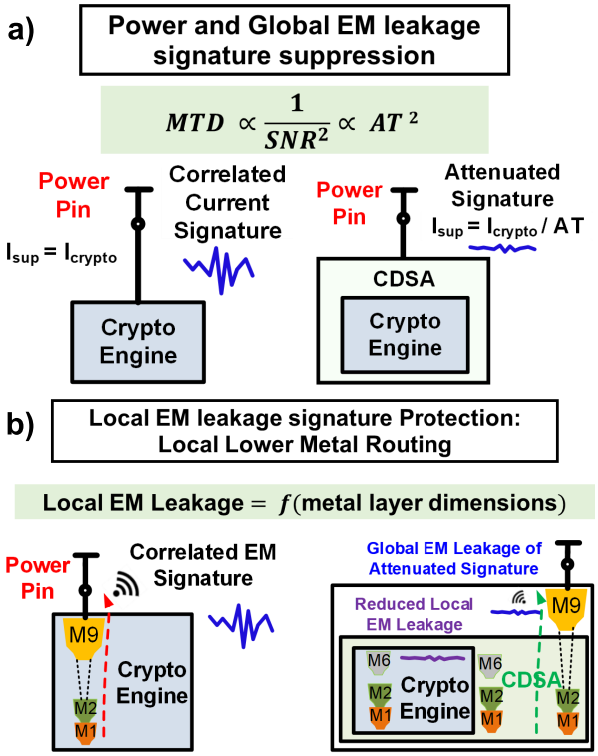



Fig. 1. Overview of the CDSA design techniques. (a) Inline current-domain signature attenuation fundamentally reduces the correlated crypto current information and provides orders of magnitude improvement in the SCA security for both power and global EM leakage. (b) Local lower level metal routing of the CDSA embedding the crypto core enables a local EM signature suppression such that the EM radiations from the higher level metal layers do not leak the critical information.

The key concepts of this article are summarized as follows.

1) CDSA technique ensures that the correlated crypto current is significantly suppressed before it reaches the supply pin, providing an $Attenuation^2$ ($AT^2$) improvement in the SCA security of cryptographic devices. It, thereby, provides resilience against both power and the "global" EM leakages.
2) Local lower metal routing technique helps in reducing the local EM SCA leakage. The idea is to suppress the critical correlated crypto signature within the lower level metal layers (up to $M_6$ in our case) before it goes through the higher metals (the root cause of the EM leakage) to connect to the external pin. Also, the CDSA hardware embedding the crypto core in the lower metals has to be "local" to minimize the IR drop.

The fabricated 65-nm CMOS test chip contains both the unprotected and protected implementations of AES-256 that

| Technique | Switched Capacitor Current Equalizer | Integrated Buck Regulator | Digital LDO with Randomization | Current Domain Signature Attenuation |
|---|---|---|---|---|
| MTD | >10M | >0.1M | 6.8M | >1B |
| Cap<br>Ind | 300pF<br>None | 3.2nF MIM<br>11.6nH (board) | 1.9nF MIM<br>None | 150pF MOS<br>None |
| Limitation | 2x Perf. Deg. | On board Inductor<br>→ Attackable | High MIM cap → EM leakage | - |

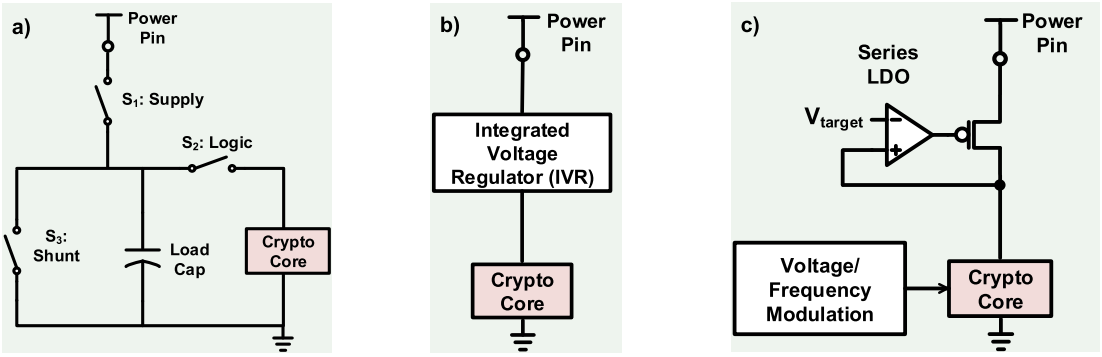



Fig. 2. State-of-the-art circuit-level countermeasures. (a) Switched capacitor current equalizer [10]. (b) IVR using buck converter with loop randomization [12]. (c) Digital LDO regulator with clock modulation [13]. The table on the top highlights the main challenges with the existing implementations. In the upcoming sections, we will see how we can achieve an MTD of 1B even with a much smaller load capacitor (150 pF), thereby reducing the area overheads.

are subjected to CPA and CEMA attacks, showing that the unprotected AES can be broken in only 8k and 12k traces, respectively, while the CDSA-AES remains protected even after 1B traces, achieving 100× higher MTD (MTD > 1B) reported to date with comparable power and area overheads.

In addition, this work, for the first time, demonstrates the effect of metal layers on the EM side-channel leakage. Using test vector leakage assessment (TVLA) methodology, it can be seen that the CDSA-AES with higher level metal routing leaks significantly more (>7×) compared with lower level metal routing, proving the effects of on-chip metal layers on EM leakage.

The remainder of this article is organized as follows. Section II summarizes the existing works on EM and power SCA countermeasures. In Section III, the circuit techniques to achieve both power and global EM SCA resilience are discussed, along with the design space exploration. Section IV presents the white-box modeling of the crypto-IC and the design considerations for local EM leakage suppression. In Section V, the system architecture is presented, along with the modes of operation. Measurement results along with the SCA analysis to evaluate the efficacy of the countermeasure are demonstrated in Section VI. Finally, Section VII concludes this article.

## II. Related Works

Power and EM SCA countermeasures can be broadly classified into three categories: logical, architectural, and physical. Logical countermeasures focus on equalizing the power consumption in each clock cycle and include sense-amplifier-based logic (SABL) [16], dual-rail precharge circuits [17], wave dynamic differential logic (WDDL) [18], and gate-level masking [19], [20]. These countermeasures usually require re-designing the library cells and also suffer from the high area and power overheads as the logic gates are replaced with a sophisticated one to mask the side-channel leakage.

The second category involves architectural countermeasures based on introducing time or amplitude-based distortions using dummy insertion, or shuffling of operations, which provides a limited enhancement in SCA security depending on the algorithm and architecture of the implementation [21].

The third and final categories include the physical circuit-level countermeasures to protect against EM and power SCA attacks. These are the most generic techniques and involve noise injection, switched capacitor-based current equalizer [10], [22], integrated voltage regulator (IVR) using buck converters [12], and digital LDO-based implementation [13]. Simulations of shunt LDO-based regulators have been recently studied and shown to be effective for power SCA resistance [23]. Noise injection-based countermeasure reduces the SNR but suffers from very high-power overheads and, hence, is not an optimum technique to enhance SCA security [24].

Switched capacitor current equalizer circuit proposed by Tokunaga and Blaauw [10] operates in three phases, as shown in Fig. 2(a). In the first phase ($S_1$ closed), the load capacitor is charged to supply. The AES core operates in the second phase ($S_2$ closed), and finally, in the third phase ($S_3$ closed), the load capacitor is discharged to a fixed bias to clear the voltage residue. Although this is a novel supply isolation technique, it has multiple tradeoffs among the size of the load capacitor (performance versus area tradeoff), the dc bias voltage (security versus power tradeoff), and the switching frequency (area versus power tradeoff), leading to a 2× performance degradation.

IVR using buck converter along with loop randomization was proposed in [12], as shown in Fig. 2(b). However, it suffers from large passives including onboard inductors, as shown in the table in Fig. 2.

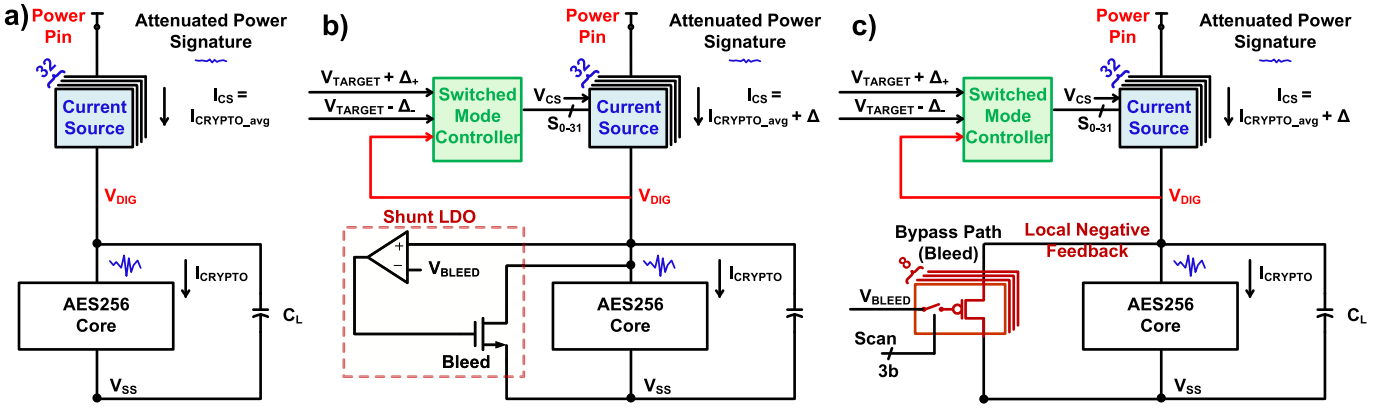



Fig. 3. Build-up to the CDSA design. (a) Ideal realization of a CS. (b) Low-bandwidth switched-mode control (SMC) loop for PVT tolerance and choosing the number of CS slices for supplying the average AES current, and the high bandwidth shunt LDO to bypass any extra current from the top that is more than the average current of the AES-256 core. (c) Shunt LDO is replaced with a PMOS bleed transistor that provides inherent negative feedback and the low-frequency regulation with much lower power and still providing the same SCA security benefits.

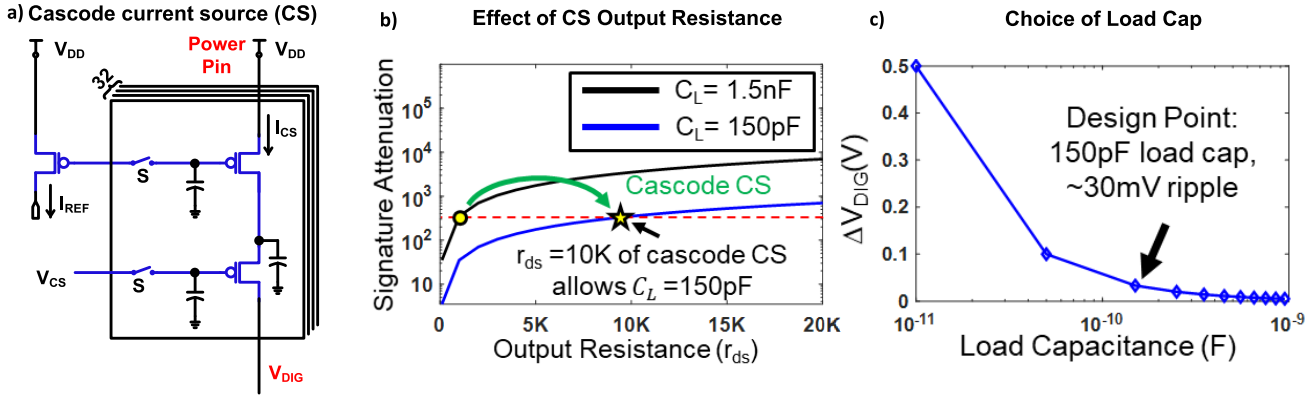



Fig. 4. Design of the constant CS. (a) Cascode CS provides (b) 10× higher output impedance compared with a simple CS implementation and, hence, (c) allows a 10× reduction in the load capacitor for iso-attenuation.

Recently, as shown in Fig. 2(c), series LDOs with noise injection along with voltage–frequency modulation were proposed to obfuscate the side-channel leakage [13]. However, it used large MIM capacitors that can leak the critical side-channel information through the higher level metal layers in the form of EM leakage. Also, ideal series LDO-based implementation inherently leaks critical information [23], as it tries to maintain a constant voltage across the crypto core, which means that the current drawn from the supply is exactly equal to the crypto current, which is undesirable for SCA resistance.

In this work, the goal is to achieve a high MTD with a lower load capacitor. By adopting the two key design techniques (refer to Section II-B), the proposed CDSA design achieves both EM and power SCA protection up to an MTD of 1B traces, thereby improving the state of the art by 100×, with a 10× lower load capacitance.

## III. Global Signature Attenuation: Concept and Circuit Design

In this section, we will study the details of the CDSA countermeasure to protect against power and global EM side-channel leakage.

### A. Concept

For an unprotected crypto engine, the supply current remains equal to the crypto current, as shown in Fig. 1(a). Our goal is to design a countermeasure such that the supply current is independent of the crypto current.

Imagine if we can somehow embed the crypto core within a CDSA hardware such that the correlated current signature is significantly suppressed (almost constant) even before it reaches the supply pin, then the MTD for power SCA would be enhanced by the square of the attenuation factor (MTD $\propto$ $AT^2$), as shown in Fig. 1(a). The MTD for EM SCA is also improved as the current flowing through higher level radiating structures (e.g., pins and board traces) is near constant. This idea of suppressing the signature in the current domain provides a huge benefit in terms of SCA security for both power and the global EM leakage.

### B. Circuit Architecture

For designing a CDSA hardware, we need the supply current to be independent of any variations in the crypto current. The first thing that comes to our mind is a constant current source (CS). However, a constant CS cannot drive a variable current load. Hence, we need a capacitor to account for the differences in the current, as shown in Fig. 3(a).

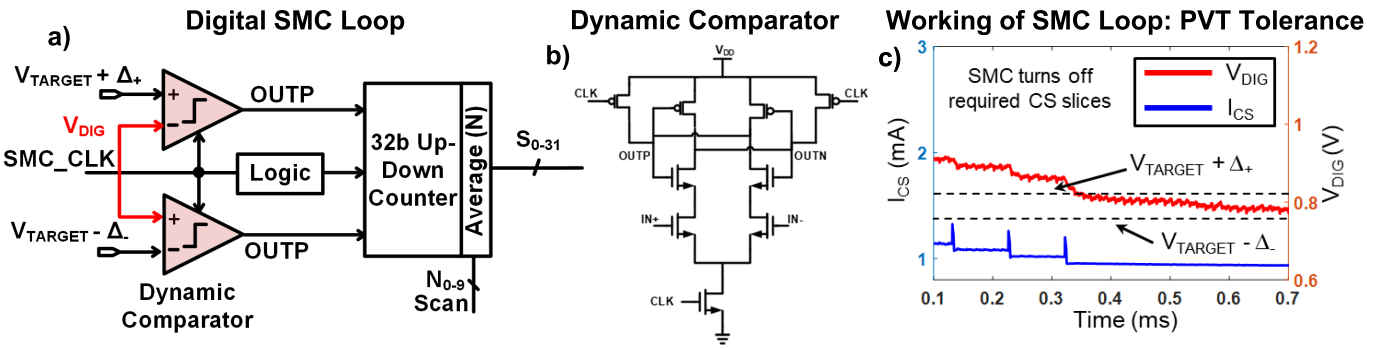



Fig. 5. (a) Design of the switched-mode control loop with guard bands. (b) Dynamic comparator checks if the $V_{\text{DIG}}$ node goes out of the guard bands. (c) SMC logic turns on or off the required number of CS slices depending on the $V_{\text{DIG}}$ voltage.

Now, as shown in Fig. 3(b), to handle the process, voltage, and temperature (PVT) variations, a low-bandwidth SMC loop is used, which tracks the $V_{\text{DIG}}$ within a guard band of $V_{\text{TARGET}} + \Delta_+$ and $V_{\text{TARGET}} - \Delta_-$ by turning on or off the required number of CS slices. The SMC loop, thus, tries to set the CS current to the average crypto current. However, due to the quantization levels of the CS, the supply current ($I_{\text{CS}}$) is set to the closest higher quantization level ($I_{\text{CRYPTO}_{\text{avg}}} + \Delta$).

Now, to drain the excess current ($\Delta$), a high-power shunt LDO [23], [25], [26] can be utilized, which senses the node $V_{\text{DIG}}$ and controls the bleed NMOS gate voltage to draw the difference of current between $I_{\text{CS}}$ and $I_{\text{CRYPTO}}$. However, the shunt loop needs to be very high bandwidth ($\sim 10\times$ more than the crypto frequency) to respond to the instantaneous changes in the load (crypto) current and, hence, would incur a high-power overhead. Instead, as shown in Fig. 3(c), a PMOS bleed path is utilized, which provides dc regulation through local negative feedback. The PMOS acts as a bypass path for the extra current ($\Delta$) and minimizes the power overhead significantly compared with the shunt loop.

### C. Cascode CS: Lower Load Capacitor

To achieve high signature attenuation (AT), we need a high output impedance CS or a high load capacitor. Hence, a cascode CS is chosen, as shown in Fig. 4(a), which provides a high output impedance ($r_{\text{ds}}$) compared with one-stack CS and allows $10\times$ lower load capacitor ($C_L$) to achieve iso-attenuation, as shown in Fig. 4(b). The CDSA utilizes digitally tunable cascode CS with high output impedance to power the AES. Although the choice of a smaller load capacitor ($C_L$) leads to voltage fluctuations ($\sim$30–50 mV) at the $V_{\text{DIG}}$ node [see Fig. 4(c)], the high output impedance of the CS stage ensures that the voltage fluctuations are not reflected to the supply current that an attacker can access.

### D. CDSA Design

As discussed in Section II, traditional LDOs inherently leak critical information [23]. For the CDSA design, the supply current does not track the AES current, and hence, the SMC loop is a low-bandwidth control loop to set the supply current to the average crypto current. Instead, we choose to tolerate

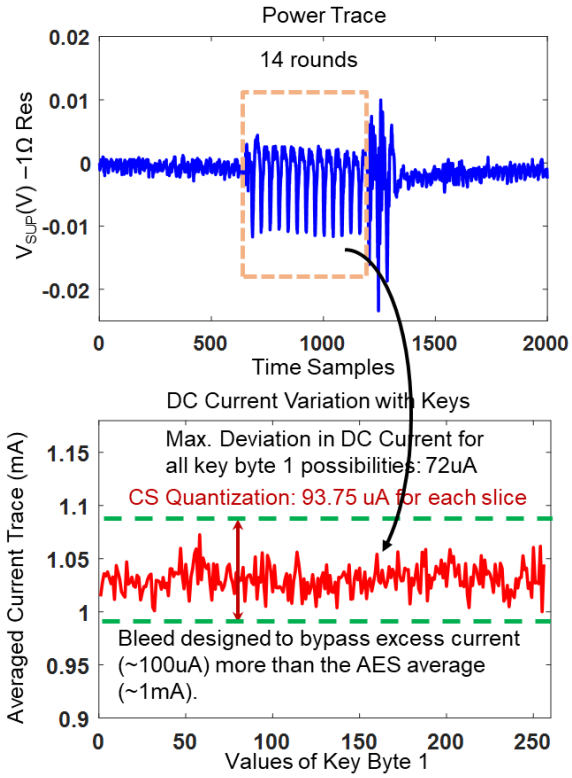



Fig. 6. (a) Sample Power trace of the AES-256 showing 14 rounds of the encryption. (b) Average current of the trace during the 14 rounds is computed for all the 256 possibilities of the first key byte. The CS quantization level (unit CS current) is designed to be higher than the maximum key-to-key variation in the average crypto current so that any key-dependent information is not leaked through the power trace.

the $\sim$30–50-mV voltage droop across the AES engine, and the high impedance ($r_{\text{ds}} > 10$ K$\Omega$) (see Fig. 2) CS on top ensures that the current fluctuation at the supply is attenuated by

$$\text{AT} = \omega_{\text{AES}} C_L r_{\text{ds}} \tag{1}$$

which evaluates to $>350\times$.

Note that although AT shows a frequency dependence, a reduction in the AES frequency ($\omega_{\text{AES}}$) would reduce the $I_{\text{AES}_{\text{avg}}}$ linearly and, hence, reduces $I_{\text{CS}}$, thereby increasing $r_{\text{ds}}$ linearly (since $r_{\text{ds}} = (1/\lambda * I_{\text{CS}})$), as the top CS is biased

in saturation. Hence, AT of the CDSA circuit remains almost constant of the crypto frequency.

Now, the goal of the CDSA circuit is to provide the average load (AES) current plus a delta current that leaks through the bypass PMOS bleed path to ground, providing local negative feedback, which leads to the ability to support any $I_{\mathrm{AES_{avg}}}$ in between two quantized current levels of the CS. Hence, the shunt-path PMOS bleed (biased for near-threshold operation) aids in low-frequency analog regulation without the need for a high-power shunt loop. The voltage at the $V_{\mathrm{DIG}}$ node is, thus, given as

$$V_{\mathrm{DIG}} = V_{\mathrm{BLEED}} + V_{T_p} + \sqrt{\frac{2\Delta}{K'_p(\frac{W}{L})_{\mathrm{BLEED}}}} \tag{2}$$

where $V_{T_p}$ represents the threshold voltage of the PMOS bleed, and $\Delta$ is the excess current (quantization error) from the supply. Hence, with a large size of the bleed PMOS, (2) gets modified as

$$V_{\mathrm{DIG}} \approx V_{T_p} + V_{\mathrm{BLEED}}. \tag{3}$$

Now, the bleed should not be very large as it would unnecessarily drain extra current from the supply, increasing the power overhead without increasing the MTD. This is discussed in detail in Section III-G. The CS consists of 32 slices of PMOS, and nominally, 16 of them are turned on. The shunt path PMOS bias (near-threshold operation) and the number of PMOS legs ON are scan controllable to analyze the effect of the extra bleed current on signature attenuation.

### *E. PVT Tolerance and SMC Loop*

The design of the SMC loop is shown in Fig. 5(a). The slow digital SMC LDO tracks and regulates the voltage across the AES ($V_{\mathrm{DIG}}$ between $V_{\mathrm{TARGET}} + \Delta_+$ and $V_{\mathrm{TARGET}} - \Delta_-$) by turning on or off the required number of PMOS CS slices. Two dynamic comparators [see Fig. 5(b)] compare $V_{\mathrm{DIG}}$ with $V_{\mathrm{TARGET}} + \Delta_+$ and $V_{\mathrm{TARGET}} - \Delta_-$, respectively, and a 32-bit up–down counter with averaging (to control the loop frequency) controls the appropriate number of CS slices to be turned on. If $V_{\mathrm{DIG}} > V_{\mathrm{TARGET}} + \Delta_+$ for $N$ SMC clock cycles, then a CS is turned on. On the other hand, if $V_{\mathrm{DIG}} < V_{\mathrm{TARGET}} - \Delta_-$ for $N$ SMC clock cycles, then a CS is turned off. Fig. 5(c) shows the working of the SMC loop where it turns off the required number of CS slices to reach the steady state ($V_{\mathrm{DIG}}$ within the guard band) after which it remains disengaged. The SMC loop can handle any PVT variations from chip-to-chip. At startup, CDSA requires $< 500\ \mu$s to settle [see Fig. 5(c)], which can be dummy operations. It should be noted that the SMC LDO is a low-BW loop (clocked at $< 10$ kHz, $V_{\mathrm{DIG}}$ output pole at $\sim$106 kHz) and has a dead band of 50 mV, such that it remains disengaged during the steady-state operation of the CDSA-AES circuit. The design of the dynamic comparators in the SMC loop that compares the $V_{\mathrm{DIG}}$ node voltage with the guard-band levels is shown in Fig. 5(c).

For the SMC loop, it needs to be noted that once the average current is set, that is, in steady state, the SMC is disengaged, and the signature attenuation is given by the output resistance of the CS and the load capacitance.

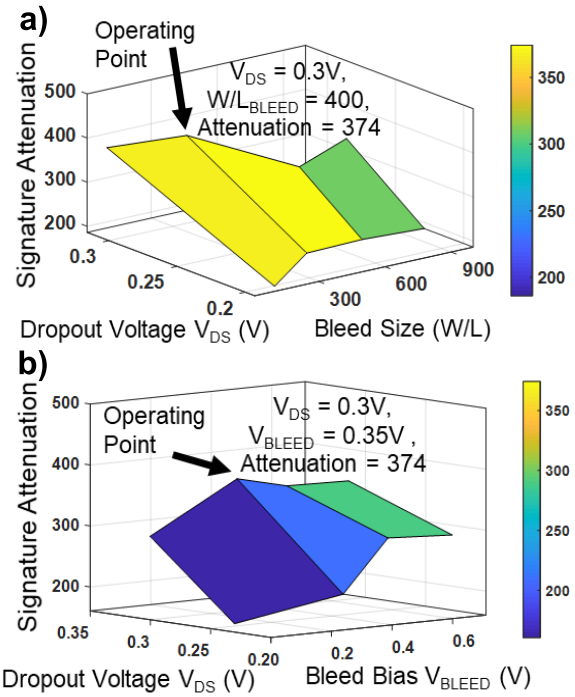



Fig. 7. CDSA design space exploration. (a) Dropout voltage ($V_{\mathrm{DS}}$) of 0.3 V across the CS and a bleed size of 400 is the most optimal choice, as a higher bleed size increases the current drawn from the supply and reduces the attenuation. (b) Bleed bias of 0.35 V is the most optimum beyond which it goes toward cutoff and the signature attenuation reduces.

### *F. Quantization Versus Key Leakage: Choice of CS Quantization*

The average crypto current is a weak function of the secret key under attack, and our goal is to ensure that any key-dependent variation is not reflected to the supply current. Hence, the quantization level is given as

$$I_{\mathrm{CS}_{N+1}} - I_{\mathrm{CS}_N} > (\delta I_{\mathrm{AES_{avg}}})_{\max} \tag{4}$$

where $(\delta I_{\mathrm{AES_{avg}}})_{\max}$ is the maximum deviation in the average AES current for all the 256 different possibilities of a key byte. Thus, the unit current ($\sim$94 $\mu$A) of the CS is chosen such that it is higher than the key-dependent variation in $I_{\mathrm{AES_{avg}}}((\delta I_{\mathrm{AES_{avg}}})_{\max} \sim 72\ \mu$A) [see Fig. 6(a) and (b)] so that the key-dependent information in average dc current is not transferred to supply current and is leaked by the bleed PMOS, making the design highly secure.

### *G. Design Space Exploration*

Design space exploration of the CDSA-AES is shown in Fig. 7(a) and (b). As the bleed bias ($V_{\mathrm{BLEED}}$) is increased from 0 to 200 mV, the bleed current is reduced, and the attenuation is increased as less current is drawn from the supply. Beyond 200 mV, as the bleed PMOS goes toward cutoff, the attenuation reduces. Hence, the design space exploration

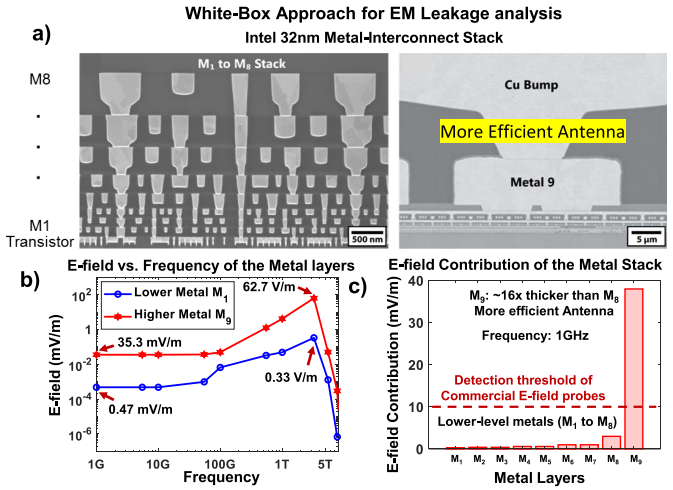



Fig. 8. EM SCA white-box analysis. (a) Intel 32-nm metal-interconnect stack showing that the higher level metals are huge compared with the lower metal layers. (b) Higher metals are thicker and, hence, act as a better antenna compared with the lower metals at the circuit-level operating frequency. (c) 3-D FEM simulations using HFSS (1 GHz, at a probe distance of 900 $\mu$m from the chip) show that the top-level metals ($M_9$ and above for the Intel 32-nm process) leak significantly more, and the radiation can be detected using the commercially available EM probes.

reveals the optimum operating point at a dropout voltage ($V_{DS}$) of 0.3 V across the CS stage and bleed bias ($V_{BLEED}$) of 0.35 V.

## IV. White-Box EM Leakage Analysis and Local Signature Suppression

Most prior works on EM SCA attacks and countermeasures treat the crypto engine as a black box, without paying much attention to the cause of the EM leakage. However, a solid understanding of the genesis of the EM leakage from a crypto-IC is necessary to develop an efficient low-overhead countermeasure.

### A. Ground-Up Analysis

As we know, the acceleration of the electrons due to the switching of the output of the digital gates creates changing electric fields and magnetic fields, leading to EM radiation, according to Maxwell's equations. Now, these generated EM fields depend on the metal layers inside the IC carrying the current, which acts as dipole antennas and radiate. These switching currents passing through the metal layers undergo a transformation to create EM radiation, and the magnitude of the fields depends on the dimensions of the metal layers. Higher level metals are considerably thicker, and hence, the EM leakage from these top metals has a higher probability of detection using the commercially available EM probes [see Fig. 8(b)]. Fig. 8(a) shows the Intel 32-nm metal-interconnect stack [27] as an example, where we see that, as we move up the metal layers, the thickness increases, and the top metal $M_9$ along with the Cu bump is huge compared with the lower metals [15]. Using a 3-D high-frequency structure simulator (HFSS) to study the $E$-field contribution of the individual metal layers, it was observed that the contribution

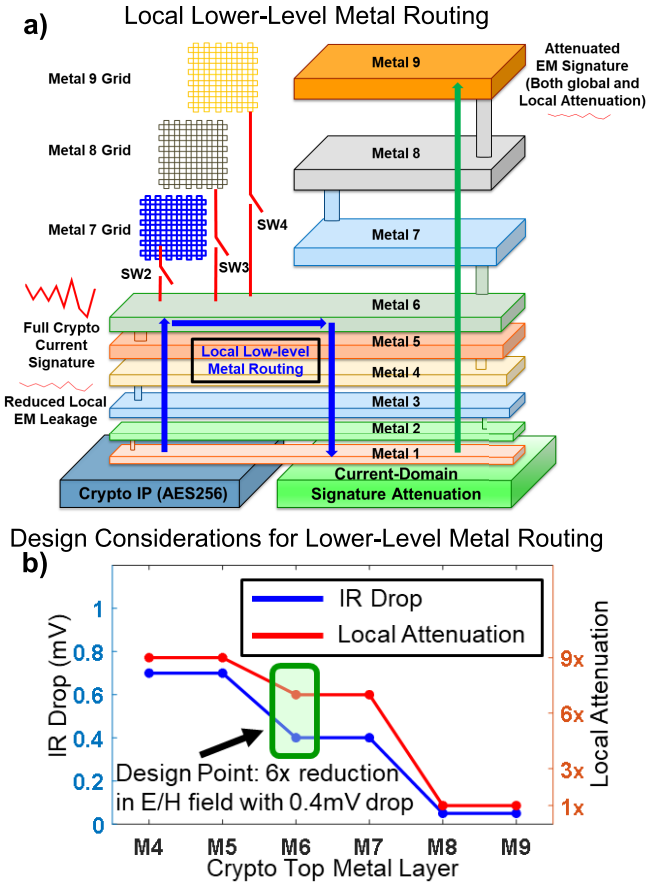



Fig. 9. CDSA design for local EM leakage suppression. (a) Crypto core is routed within the lower level metal layers and embedded within the locally routed CDSA, which attenuates the crypto signature significantly before it passes through the higher level metal layers whose leakage can be detected by an external attacker. A mesh of metal layers 7–9 is designed to evaluate the effect of higher level metal layers on the EM radiation and SCA leakage. (b) Lower level routing is performed up to metal $M_6$ considering the IR drop in the $V_{DIG}$ node. The IR drop is shown considering a routing length of 100 $\mu$m.

of the metal layers $M_9$ and above is detectable using the commercially available EM probes, and hence, these higher level metal layers are vulnerable to EM side-channel leakages [see Fig. 8(c)]. The exact metal layer above which the fields are detectable will highly depend on the process and the sensing probe used. Moreover, the ratio of electric/magnetic field strength reduction by routing through a lower metal layer would also be heavily process technology dependent. However, the key takeaway is that the top metal layers that are larger leak significantly more compared with the lower level metal layers and, hence, should not be used to route the unsuppressed correlated signature.

Through 3-D finite element method (FEM) simulation of metal traces using HFSS, it is validated that the EM leakage is a strong function of the metal dimensions carrying the correlated current [15]. Hence, the goal for EM SCA resilience is not to pass the correlated current through the higher level metal layers. However, even if the sensitive signals are routed locally, power has to be routed to the external pins through higher metals. For only power SCA protection, we can utilize the

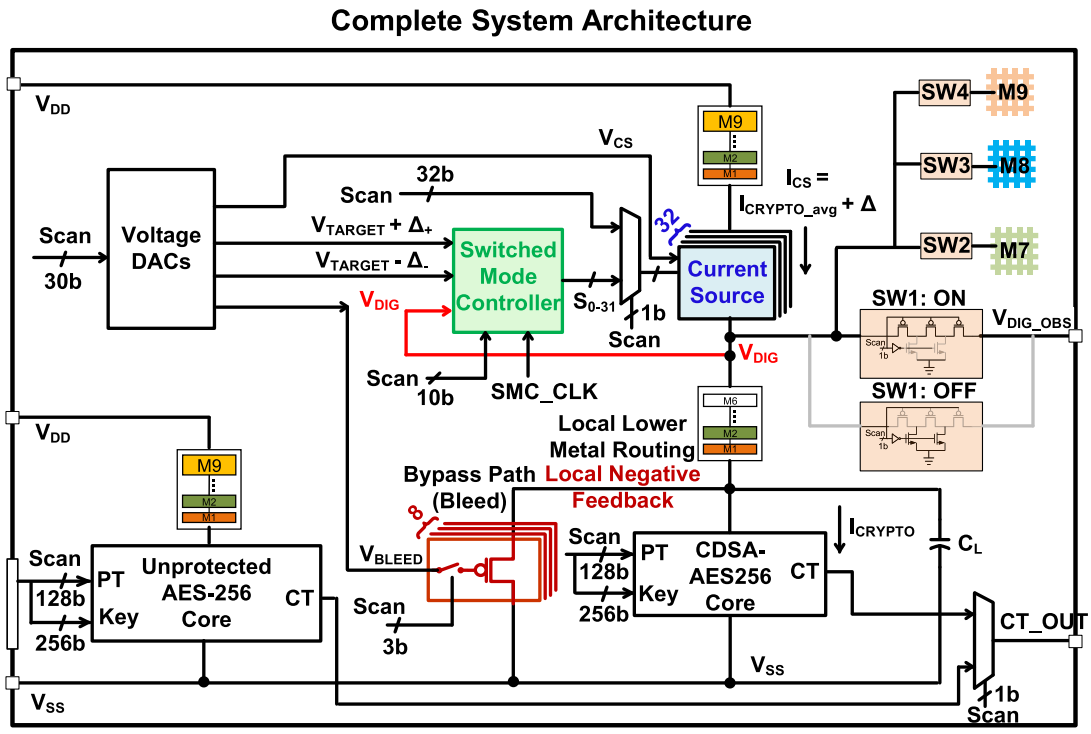



Fig. 10. Complete system architecture showing the unprotected AES-256 and the protected CDSA-AES256 cores. Highly isolating switch SW1 is designed to observe the $V_{DIG}$ voltage across the AES-256. Other switches SW2–SW4 are designed to connect the AES core to the top metal mesh structures to evaluate the effect of higher metal layers on the EM SCA leakage.

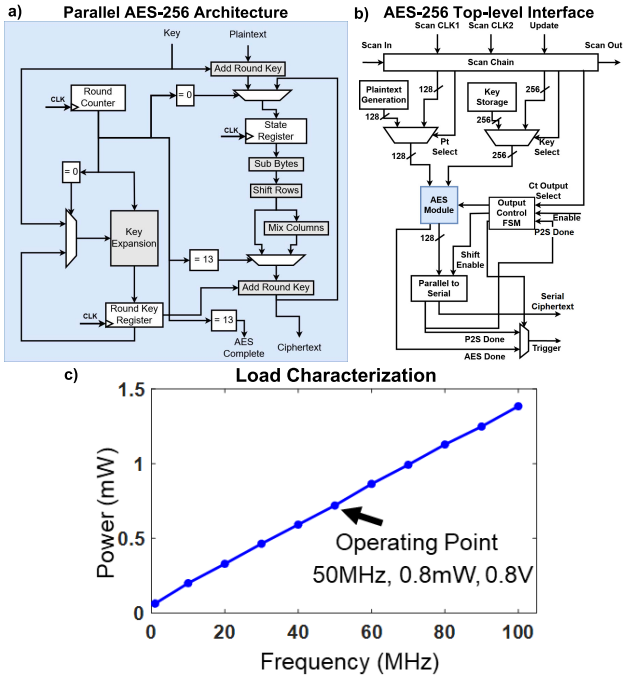



Fig. 11. (a) Parallel AES-256 architecture. (b) Top-level interface. (c) AES-256 is powered at 0.8 V at 50 MHz and consumes 0.8-mW power.

CDSA hardware to suppress the correlated current signature, but, if the routing is through the higher metals, it would still radiate and would be vulnerable to EM SCA.

Equipped with this "white-box" understanding of the genesis of the EM leakage and noting that the correlated current is the source of both power (at supply pin) and EM leakage (radiation through the current path), this work embraces CDSA with local lower level metal routing as a low-overhead generic countermeasure against both EM and power side-channel attacks. Hence, we route the crypto engine within the lower level metal layers and embed it locally within the CDSA hardware, which suppresses the signature significantly before passing it through to the top-level metal layers.

### *B. CDSA Design for EM SCA Protection: Local Lower Level Metal Routing*

The previous technique of active inline current-domain signature suppression protects against power and the global EM leakage. Here, we will look into the design strategy to prevent local EM leakage.

As shown in Fig. 9(a), the crypto-IP (AES-256 for this work) is routed within the lower level metal layers ($M_1$–$M_6$), and then, the correlated current is passed through the physically close CDSA block that is also routed locally within the lower metals. The arrows in the figure indicate the direction of flow of the current. The correlated local EM leakage is significantly suppressed by the CDSA within the lower metal layers (up to $M_6$), and it is then passed through the higher level metal layers to connect to the pin. A mesh of metals 7–9 is designed on top of the crypto core to evaluate the contribution of the top metal layers to EM radiation.

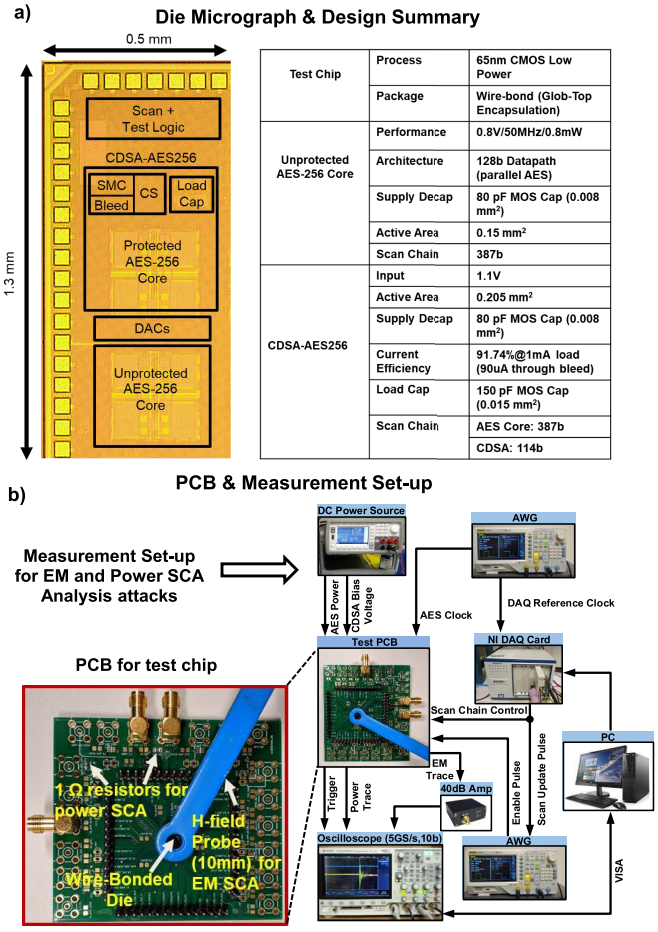



Fig. 12. (a) Die micrograph of the system in 65-nm CMOS process and design summary. (b) PCB and the measurement setup for EM and power SCA attacks.

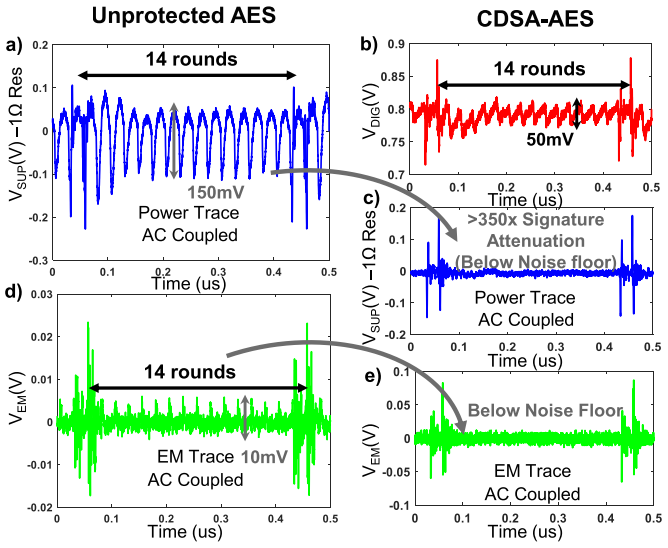



Fig. 13. Time-domain measurement results. (a) Power trace from the unprotected AES-256 clearly shows the 14 rounds of the encryption. (c) Power trace has an amplitude of 150 mV, which is significantly attenuated by a factor of $>350\times$, and the power trace for the CDSA-AES256 remains below the noise floor. (b) Intermediate node $V_{\mathrm{DIG}}$ still shows the 14 encryption rounds; however, it is only for observability and is inaccessible to an attacker. The high output impedance of the CS stage on top ensures that the fluctuation at the $V_{\mathrm{DIG}}$ is highly suppressed at the supply pin available to an attacker. Unprotected EM trace clearly shows the 14 rounds of (d) AES-256; however, for (e) CDSA-AES256, the EM trace is below the noise floor.

Lower metal routing (up to $M_6$) provides a local attenuation of $\sim 7\times$ (compared with passing the signature directly to $M_9$, which has larger dimensions and radiates more). The local routing of the CDSA with lower level metal layers has tradeoffs with the IR-drop, as shown in Fig. 9(b). Routing the $V_{\mathrm{DIG}}$ node with $M_6$ ensures that the additional IR-drop is limited to $<0.4$ mV. The load capacitor ($C_L$) uses only MOS cap (lower metal layers) rather than MIM (top metal layers) so that the EM radiation is minimized. This comes at the expense of some extra area and leakage power of the MOS cap (compared with MIM cap), which is a fundamental tradeoff to ensure high EM SCA protection. For EM SCA, MIM capacitors should never be used on the correlated current node, as the MIM capacitor plate with the correlated sensitive signature effectively turns into a radiating element, leaking critical correlated information.

## V. System Architecture

The full system architecture is shown in Fig. 10(a). It consists of both unprotected and protected AES-256 implementations. The architecture of the parallel AES-256 is shown in Fig. 11(a). AES-256 is implemented with parallel datapaths to provide high performance and requires 14 cycles per encryption. The top-level interface for external programmability and observability is shown in Fig. 11(b). To verify the correct working of the AES-256, we have an output CT (CT Serial Out) mode, where the CT is streamed out serially, as shown in Fig. 14.

TABLE I
Modes of Operation of the Crypto Cores

| Modes | Description | Configurability |
|---|---|---|
| Mode 1 | Unprotected AES256 | Separate Core |
| Mode 2 | CDSA-AES256 with higher metal routing (only power protection) | SW2-4 ON (see Fig. 2) |
| Mode 3 | CDSA-AES256 with local lower metal routing (both EM and power protection) | SW1 OFF, SW2-4 OFF (see Fig. 2) |

As seen from Fig. 10(a), the CDSA-AES has scan-controlled highly isolating switches (SW1) to connect the $V_{\mathrm{DIG}}$ node to an external pin for observability (SW1 ON) or disconnect without leaking EM during normal operations (SW1 OFF). Similar highly isolating switches (SW2–4) are kept on top of the crypto core for the protected implementation to analyze the effect of higher level metals on the EM leakage.

The system has three modes of operation, as shown in Table I. In mode 1, the unprotected AES-256 is operated.

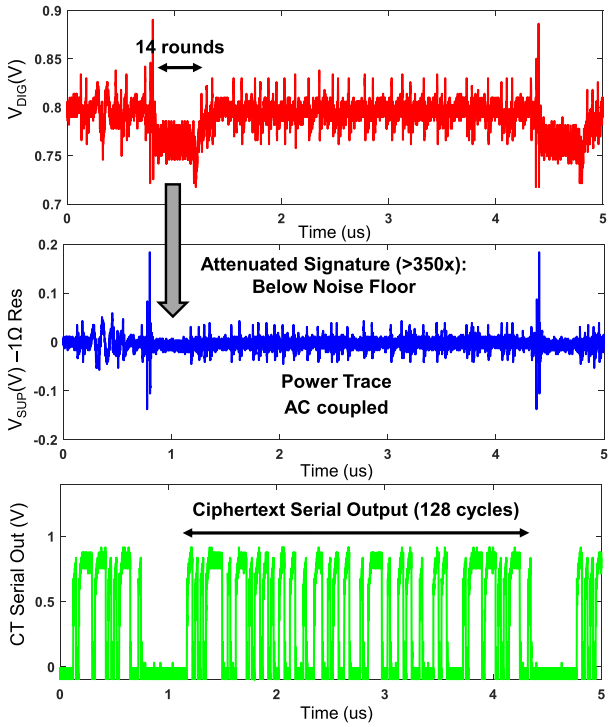



Fig. 14. AES-256 can operate in a CT serial output mode (CT Serial Out), where it outputs the 128-bit CT in 128 cycles after the 14 rounds of the encryption.

Mode 2 is the CDSA-AES with higher level metal routing (power protected), and mode 3 (default operation mode) is the fully protected implementation with lower metal routing and provides both EM and power SCA protection.

## VI. Measurement Results: Efficacy of the Countermeasure

The die micrograph of the test chip fabricated in TSMC 65-nm technology is shown in Fig. 12(a). The package was wire-bonded on the PCB with glob-top encapsulation and consumes an active area of 0.15 mm$^2$.

The PCB and measurement setup is shown in Fig. 12(b). For power SCA attacks, we mount 1-Ω resistors at the power supply of both the unprotected and protected AES-256. A 10-mm loop diameter H-field probe is used to measure the EM leakage from the IC while performing encryption. For our EM measurements, we had compared with Tekbox probes of 5, 10, and 20 mm [28], and the 10-mm probe was the most optimal choice as it picked the most EM signal. The measurement setup consists of an oscilloscope for capturing the traces and is connected through an external 40-dB wideband amplifier for the EM trace capture.

The unprotected AES is powered with 0.8-V input and consumes ∼1-mA average current at 50 MHz, as shown in Fig. 11(c).

### A. Time-Domain Measurement Results

Fig. 13 shows the time-domain measurement results for both the unprotected and protected AES-256. The power trace

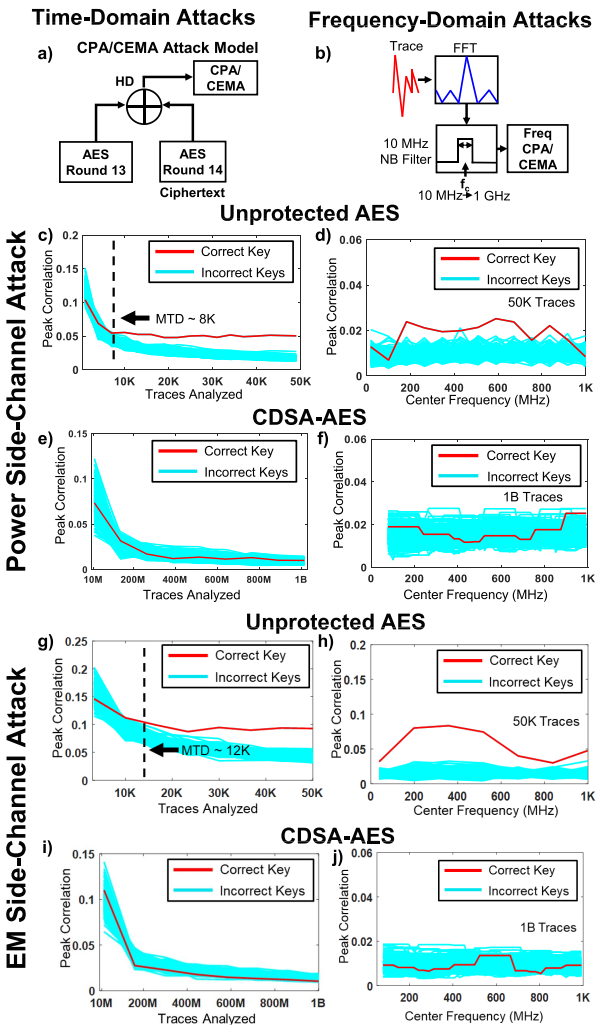



Fig. 15. EM and power SCA attack evaluation. (a) Attack model for CPA/CEMA uses the HD between the CT and the output of the 13th round. A time-domain attack is performed by analyzing the correlation for each time sample of the traces. (b) Frequency-domain CPA/CEMA is performed by performing an FFT on the power/EM traces. The time-domain traces are passed through an NB filter of 10-MHz bandwidth, and the center frequency is varied from 10 MHz to 1 GHz. (c) Time-domain CPA on the unprotected AES-256 traces shows that the correct key can be recovered within 8k traces, while(e) the protected implementation could not be broken even after 1B encryptions. (d) Frequency-domain CPA on the unprotected AES reveals that the correct key shows up with 50k traces, while (f) protected AES remains secure even after 1B traces. (g) Time-domain CEMA on the unprotected AES shows an MTD of 12k, while (i) protected CDSA-AES could not be broken even with 1B measurements. (h) Frequency-domain CEMA on the unprotected AES-256 breaks the correct key within 50k traces, while (j) protected implementation remains secure even after 1B traces.

for the unprotected AES clearly shows the 14 rounds of the encryption, which is ∼150 mV in amplitude, while the CDSA-AES power signature is attenuated by >350× and remains below the noise floor of the oscilloscope. Observing the $V_{DIG}$ across the AES engine, we can see the 14 rounds of the AES; however, we choose to tolerate these fluctuations at $V_{DIG}$ with a smaller $C_L$ to reduce area overhead and, instead, have the high impedance ($r_{ds}$) CS on top, which ensures that the correlated signatures are not reflected to the supply current, as seen from Fig. 13. Also, for the EM signature, the 14 rounds are clearly visible for the unprotected

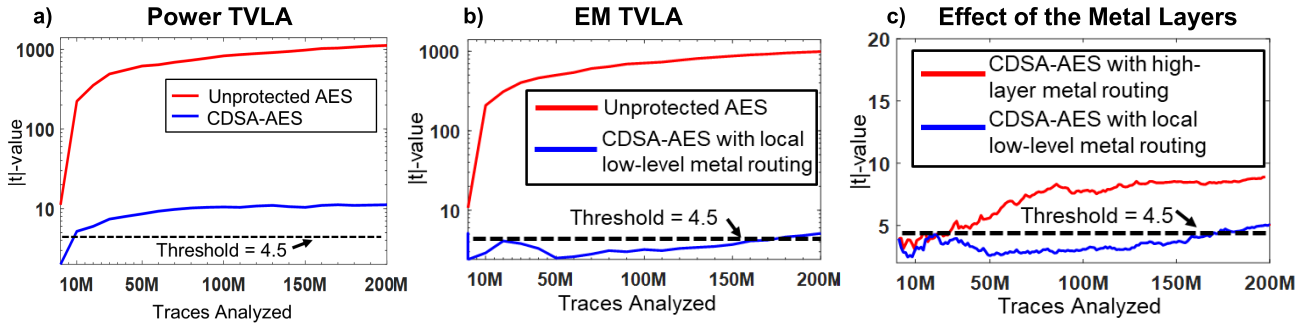



Fig. 16. Power and EM fixed versus random TVLA. (a) Unprotected AES-256 has a $t$-value of $>1000$ with 200M analyzed power traces, while it remains $\sim$10 for the CDSA-AES256. (b) EM TVLA on the unprotected AES-256 shows a $t$-value of $>1000$, while the $t$-value protected implementation (mode 3, with lower metal routing) remains $\sim$5 for 200M analyzed traces. (c) CDSA-AES with higher level metal routing shows $>7\times$ higher leakage compared with the lower level routing, as it crosses the $t$-value threshold of 4.5 within 20M traces in mode 2, while the fully protected implementation (mode 3) crosses the threshold in 170M traces.

TABLE II
COMPARISON WITH STATE OF THE ART

| Parameter | | | This Work | JSSC'20 [13] | JSSC'18 [12] | JSSC '10 [10] | VLSI'15 [11] |
|---|---|---|---|---|---|---|---|
| Countermeasure Technique | | | Current Domain Signature Attenuation | Digital LDO with randomization | Integrated Buck Regulator | Switched Capacitor Current Equalizer | Charge Recovery Logic |
| Process | | | 65nm CMOS | 130nm CMOS | 130nm CMOS | 130nm CMOS | 65nm CMOS |
| Crypto Algorithm | | | AES-256 | AES-128 | AES-128 | AES-128 | AES-128 |
| Standalone AES Power/Frequency | | | 0.8mW @ 50MHz, 0.8V | 10.9mW @ 80MHz, 0.84V | 10.5mW @ 40MHz | 33mW @ 100MHz | 138mW@1.32 GHz |
| Design Overheads | Area | | 36.7%[c] | 36.9%[b] | 1%[a] | 33% | 25% |
| | Capacitor | | 150pF MOS | 1.9nF MIM | 3.2nF MIM | 300pF | - |
| | Power | | 49.8%[c] | 32% | 5%*[a] | 20% | 30% |
| | Perf. | | 0% | 10.4% | 3.33% | 50% | 0% |
| SCA Analysis | Time/Freq Domain | | Time, Freq | Time, Freq | Time, Freq | Time | Time |
| | MTD | Power | **>1B (>125,000x)** | 8M (4210x) | >100K (20x) | >10M (2500x) | 940K (251x) |
| | | EM | **>1B (>83,333x)** | 6.8M (136x) | - | - | - |
| | Attack Mode | | Power/EM | Power/EM | Power | Power | Power |

[a]Does not include regulator area/power, [b]Does not include MIM Cap area, [c]Power overhead includes the dropout voltage across CS, the excess bleed current drawn during the steady-state operation, as well as the $V_{DIG}$ guard-banding to ensure no performance degradation. Area overhead includes the load cap area, CS, SMC loop, and the bleed path.

implementation, while it remains below the noise floor for the CDSA-AES.

Both the unprotected and protected AES-256 can be operated in the CT Serial Out Mode, as shown in Fig. 14. In this mode, the 128-bit CT is serially output after the 14 cycles of each encryption.

### B. EM and Power SCA and Attacks

Now, let us look into the SCA resiliency of the unprotected and protected implementations. Both time- and frequency-domain CPA and CEMA are performed. TVLA is also shown for both unprotected and protected implementations.

*1) Attack Model:* For both CPA/CEMA attacks, we use the HD model of the last two rounds (HD between the CT and the output of the 13th round) of the AES-256. For the frequency-domain attack, the traces are passed through an NB filter of 10-MHz bandwidth with the center frequency sweeping from 10 MHz to 1 GHz (see Fig. 15).

*2) CPA Attacks and Power-TVLA:* Fig. 15 shows the HD attack model used between the last two rounds of AES (13th round output and the CT), and a correlational power attack (CPA) on the unprotected AES implementation shows an MTD of 8k, while the CDSA-AES cannot be broken even after 1B traces (without any intentional noise injection). While

all key bytes show similar trends, we demonstrate the efficacy of the countermeasure with attacks on the first key byte. Fixed versus random TVLA on the unprotected AES shows a $t$-value of 1056 after 200M traces compared with ∼12 for CDSA-AES [Fig. 16(a)]. Frequency-domain CPA with windowed fast Fourier transform (FFT) has been performed with a window size of 10 MHz, and the center frequency is swept from 10 MHz to 1 GHz. However, the correct key byte was not revealed for any frequency band, even after 1B traces, showing an MTD improvement of ∼125 000×.

*3) CEMA Attacks and EM-TVLA:* CEMA on the unprotected AES shows an MTD of ∼12 K, while the CDSA-AES is not broken after 1B measurements (see Fig. 15). The results were also verified with frequency-domain CEMA. TVLA on the unprotected AES shows a $t$-value of 961 compared with a $t$-value of 6 for the CDSA-AES [with lower metal routing—Mode 3: Fig. 16(b)]. The effect of higher metal layer routing on EM leakage is analyzed by turning on highly isolating switches (SW2–SW4) that connect $V_{\mathrm{DIG}}$ to higher metal radiating structures (see Fig. 2). In this Mode (2), with all M7–M9 connected, the EM leakage crosses the threshold of 4.5 within 20M traces compared with ∼170M traces for Mode 3, demonstrating the effect of local attenuation (>7×) and the significance of the local lower metal routing for EM SCA protection [Fig. 16(c)].

Note that since CDSA fundamentally involves active SNR reduction in the current/voltage domain as a countermeasure, the power and EM traces are sufficiently averaged (10 000×) for the SCA attack to enhance the SNR. In the future, we will explore and evaluate the optimal averaging versus the number of unique traces required to mount the best possible attack.

### C. Comparison With State of the Art

Compared with the existing state-of-the-art circuit-level countermeasures, CDSA with lower level metal routing provides 100× higher MTD (see Fig. 17) with comparable power and area overheads (see Table II). CDSA-AES has been evaluated against both time- and frequency-domain attacks for power and EM SCA. This is also a generic countermeasure and can be extended to any other crypto engines without any performance degradation.

It should be noted that this IC is designed in the 65-nm process, while some of the previous works were performed in 130-nm CMOS technology. At lower technologies, the supply voltage ($V_{DD}$) is lower, and the output resistance ($r_{\mathrm{ds}}$) of a transistor gets reduced. To achieve the same $r_{\mathrm{ds}}$, the size of the CS has to be enhanced, leading to an increase in the area overheads for 65 nm compared with the 130 nm. Also, since the VDD is lower, for iso-dropout voltage ($V_{\mathrm{DS}}$), the power overhead would be increased at 65 nm compared with the 130 nm. In addition, the average load current of the crypto core ($I_{\mathrm{CRYPTO_{avg}}}$) is also reduced, and hence, the power overhead would be worse at 65 nm. Overall, the design tradeoffs at the 65-nm node are worse compared with the 130-nm CMOS process. Hence, as we scale down technologies, we need more scalable circuits, and hence, digital-friendly implementation of the CDSA should be developed, which is a part of the future work.

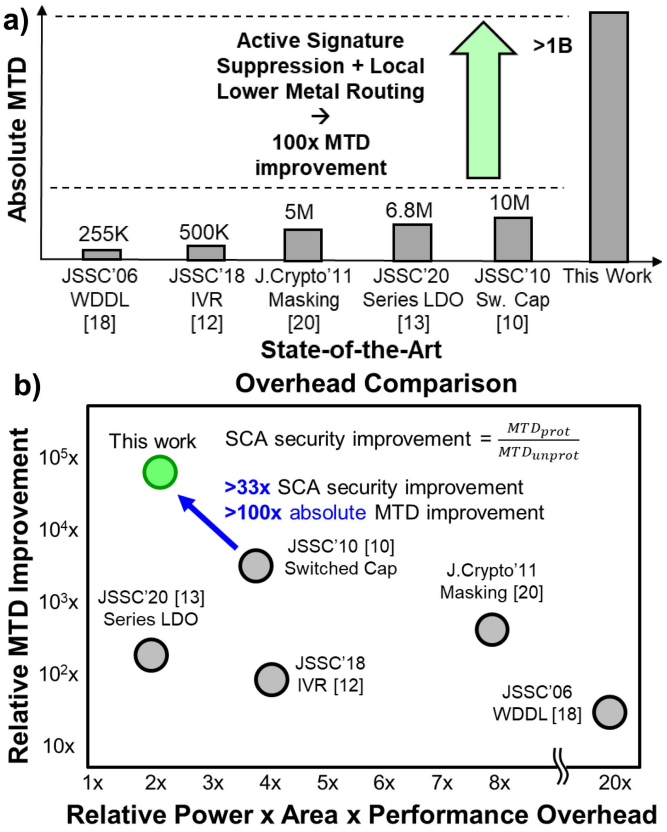



Fig. 17. Summary. (a) Utilizing active signature attenuation and local lower metal routing, CDSA achieves 100× improvement in SCA protection over the state of the art. (b) Overhead comparison with the previous works.

## VII. Conclusion

The proposed countermeasure provides both power and EM SCA immunity utilizing in-line active signature suppression and local lower level metal routing leading to a 100× MTD improvement over the state of the art [see Fig. 17(a) and (b)]. CDSA-AES256 achieves >1B MTD against CPA and CEMA attacks, which is an improvement of >125 000× and 83 333×, respectively, compared with the unprotected implementation. It is a low-overhead countermeasure and incurs a power overhead of 49% and an area overhead of 36%. The power overhead is mainly due to the dropout voltage across the CS, and the area overhead is due to the restriction that we use only MOS capacitors instead of MIM, which are implemented in the higher metal layers and can leak critical information. Finally, the presented CDSA hardware is a generic countermeasure and can be extended to any crypto algorithm as a wrapper around it (useful for legacy protection), without any performance penalty.

## References

[1] P. C. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proc. 19th Annu. Int. Cryptol. Conf. Adv. Cryptol. (CRYPTO)*, Santa Barbara, CA, USA, Aug. 1999, pp. 388–397.

[2] D. Genkin, L. Pachmanov, I. Pipman, and E. Tromer, "ECDH key-extraction via low-bandwidth electromagnetic attacks on PCs," in *Proc. RSA Conf. Cryptographers' Track (CT-RSA)*, LNCS 9610. Springer, 2016, pp. 219–235.
[3] C. Paul Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems," in *Advances Cryptology* (Lecture Notes in Computer Science). Berlin, Germany: Springer, 1996, pp. 104–113.
[4] D. Das, A. Golder, J. Danial, S. Ghosh, A. Raychowdhury, and S. Sen, "X-DeepSCA: Cross-Device Deep Learning Side Channel Attack," in *Proc. 56th ACM/IEEE Des. Automat. Conf. (DAC)*, Jun. 2019, pp. 1–6.
[5] A. Golder, D. Das, J. Danial, S. Ghosh, S. Sen, and A. Raychowdhury, "Practical approaches toward Deep-Learning-Based cross-device power side-channel attack," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 27, no. 12, pp. 2720–2733, Dec. 2019.
[6] P. Kocher, J. Jaffe, B. Jun, and P. Rohatgi, "Introduction to differential power analysis," *J. Cryptograph. Eng.*, vol. 1, no. 1, pp. 5–27, Apr. 2011.
[7] *TEMPEST Attacks Against AES*, Fox-IT, Fremont, CA, USA, 2008.
[8] E. Brier, C. Clavier, and F. Olivier, "Correlation power analysis with a leakage model," in *Proc. 6th Int. Workshop Cryptograph. Hardw. Embedded Syst. (CHES)*, Cambridge, MA, USA, Aug. 2004, pp. 16–29.
[9] C. O'Flynn, "A framework for embedded hardware security analysis," Ph.D. dissertation, Dalhousie Univ., Halifax, NS, Canada, 2017. [Online]. Available: http://hdl.handle.net/10222/73002
[10] 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.
[11] S. Lu, Z. Zhang, and M. Papaefthymiou, "1.32GHz high-throughput charge-recovery AES core with resistance to DPA attacks," in *Proc. Symp. VLSI Circuits (VLSI Circuits)*, Jun. 2015, pp. 1–9.
[12] 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.
[13] 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.
[14] D. Das, J. Danial, A. Golder, and N. Modak, "27.3 EM and power SCA-resilient AES-256 in 65nm CMOS through> 350 current-domain signature attenuation," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2020, pp. 424–426.
[15] D. Das, M. Nath, B. Chatterjee, S. Ghosh, and S. Sen, "STELLAR: A generic EM side-channel attack protection through ground-up root-cause analysis," in *Proc. IEEE Int. Symp. Hardw. Oriented Secur. Trust (HOST)*, May 2019, pp. 11–20.
[16] 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. Eur. Solid-State Circuits (ESSCIRC)*, Sep. 2002, pp. 403–406.
[17] M. Bucci, L. Giancane, R. Luzzi, and A. Trifiletti, "Three-phase dual-rail pre-charge logic," in *Cryptographre Hardware Embedded Systems* (Lecture Notes in Computer Science). Berlin, Germany: Springer, 2006, pp. 232–241.
[18] D. D. Hwang *et al.*, "AES-based security coprocessor IC in 0.18um CMOS with resistance to differential power analysis side-channel attacks," *IEEE J. Solid-State Circuits*, vol. 41, no. 4, pp. 781–792, Apr. 2006.
[19] T. Popp, M. Kirschbaum, T. Zefferer, and S. Mangard, "Evaluation of the masked logic style MDPL on a prototype chip," in *Cryptographre Hardware Embedded Systems* (Lecture Notes in Computer Science). Berlin, Germany: Springer, Sep. 2007, pp. 81–94.
[20] 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.
[21] 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. 065009.
[22] A. Shamir, "Protecting smart cards from power analysis with detachable power supplies," U.S. Patent 6 507 913 B1, Jan. 14, 2003. [Online]. Available: https://patents.google.com/patent/US6507913B1/en
[23] 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, Oct. 2018.
[24] D. Das, S. Maity, S. B. Nasir, S. Ghosh, A. Raychowdhury, and S. Sen, "High efficiency power side-channel attack immunity using noise injection in attenuated signature domain," in *Proc. IEEE Int. Symp. Hardw. Oriented Secur. Trust (HOST)*, May 2017, pp. 62–67.
[25] T. Musah *et al.*, "A 4–32 Gb/s bidirectional link with 3-Tap FFE/6-tap DFE and collaborative CDR in 22 nm CMOS," *IEEE J. Solid-State Circuits*, vol. 49, no. 12, pp. 3079–3090, Dec. 2014.
[26] S. B. Nasir, S. Sen, and A. Raychowdhury, "A 130nm hybrid low dropout regulator based on switched mode control for digital load circuits," in *Proc. 42nd Eur. Solid-State Circuits Conf.*, Sep. 2016, pp. 317–320.
[27] S. Natarajan *et al.*, "A 32nm logic technology featuring 2nd-generation high-k + metal-gate transistors, enhanced channel strain and 0.171 x03BC;m2 SRAM cell size in a 291Mb array," in *IEDM Tech. Dig.*, Dec. 2008, pp. 1–3.
[28] Tekbox Digital Solutions, Singapore. *TBPS01 EMC Near-Field Probes*. Accessed: Oct. 2020. [Online]. Available: https://www.tekbox.com/product/tekbox-tbps01-emc-near-field-probes/

**Debayan Das** (Member, IEEE) received the Bachelor of Electronics and Telecommunication Engineering degree from Jadavpur University, Kolkata, India, in 2015. He is currently pursuing the Ph.D. degree in electrical and computer engineering with Purdue University, West Lafayette, IN, USA, working with Prof. Shreyas Sen.

Prior to joining 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, Hillsboro, OR, USA, over the summers of 2018 and 2020. His research interests include mixed-signal IC design and hardware security.

Mr. Das was a recipient of the IEEE HOST Best Student Paper Award in 2017 and 2019, and the Third Best Poster Award in the IEEE HOST 2018. In 2019, one of his papers was recognized as a Top Pick in Hardware and Embedded Security published over the span of the last six years. He was recognized as the winner (third place) of the ACM ICCAD 2020 Student Research Competition (SRC). During his Ph.D., he has been awarded the ECE Fellowship during 2016–2018, and the Bilsland Dissertation Fellowship during the final year (2020–2021) for his outstanding overall achievements.

**Josef Danial** received the B.Sc. degree in computer engineering from Purdue University, West Lafayette, IN, USA, in 2018, where he is currently pursuing the master's degree with the SPARC Lab as a Graduate Research Assistant.

He has two years of industry experience in automotive (Fiat Chrysler Automobiles) and IOT (Cisco Jasper) companies. His research interests include machine learning, hardware security, and computer vision.

**Anupam Golder** (Graduate Student Member, IEEE) received the B.Sc. degree in electrical and electronic engineering from the Bangladesh University of Engineering and Technology (BUET), Dhaka, Bangladesh, in 2015. He is currently pursuing the Ph.D. degree with the Georgia Institute of Technology, Atlanta, GA, USA.

He is a Graduate Research Assistant at Integrated Circuits and Systems Research Laboratory (ICSRL). His research interests include side-channel analysis of software and hardware implementations of cryptographic algorithms using machine learning, and hardware accelerator design for post-quantum cryptographic schemes.

**Nirmoy Modak** (Graduate Student Member, IEEE) received the B.E. degree in electronics and telecommunication engineering from Jadavpur University, Kolkata, India, in 2012, and the M.Tech. degree in electrical engineering from IIT Bombay, Mumbai, India, in 2015. He is currently pursuing the Ph.D. degree in electrical engineering with Purdue University, West Lafayette, IN, USA.

He was an Electrical Design Engineer at Cypress Semiconductor Pvt. Ltd., Bengaluru, India, from 2015 to 2016. He is currently an Assistant Professor with Jadavpur University. His research interests include the design of circuits and systems for human body communication and mixed-signal circuit design.

**Shovan Maity** (Graduate Student Member, IEEE) received the Ph.D. degree in electrical engineering from Purdue University, West Lafayette, IN, USA, in 2019.

Currently, he is working as a Senior Circuit Design Engineer at Qualcomm, San Diego, CA, USA. Previously, he worked as an Analog Design Engineer at Intel, Bengaluru, India, from 2014 to 2016. His research interest lies in the area of mixed-signal circuits and systems for the Internet of Things, biomedical, and security applications.

**Baibhab Chatterjee** (Graduate Student Member, IEEE) received the B.Tech. degree in electronics and communication engineering from the National Institute of Technology (NIT), Durgapur, India, in 2011, and the M.Tech. degree in electrical engineering from IIT Bombay, Mumbai, India, in 2015. He is currently pursuing the Ph.D. degree with the School of Electrical Engineering, Purdue University, West Lafayette, IN, USA.

His industry experience includes two years as a Digital Design Engineer/a Senior Digital Design Engineer with Intel, Bengaluru, India, and one year as a Research and Development Engineer with Tejas Networks, Bengaluru. His research interest includes low-power analog, RF, and mixed-signal circuit design for secure biomedical applications.

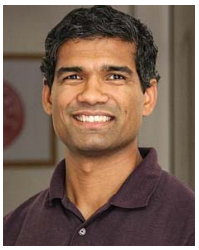
Mr. Chatterjee received the University Gold Medal from NIT, Durgapur, India, in 2011, the Institute Silver Medal from IIT Bombay in 2015, the Andrews Fellowship at Purdue University during 2017–2019, the HOST 2018 Best Student Poster Award (Third), the CICC 2019 Best Paper Award (overall), and the RFIC/IMS 2020 3MT Award (audience choice).

**Dong-Hyun Seo** received the B.S. degree in electronics and radio engineering from Kyung Hee University, Yongin, South Korea, in 2013, and the M.S. degree in electronics computer engineering from Hanyang University, Seoul, South Korea, in 2015. He is currently pursuing the Ph.D. degree with the School of Electrical Engineering, Purdue University, West Lafayette, IN, USA.

His research interest includes CMOS low-power analog, mixed-signal, and RF integrated circuit design for sensor node interfacing.

**Muya Chang** (Graduate Student Member, IEEE) is currently pursuing the Ph.D. degree in electrical and computer engineering (ECE) with Georgia Tech, Atlanta, GA, USA.

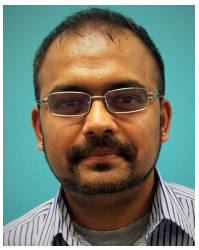
He is a member of the Integrated Circuits and Systems Research Lab and is advised by ECE Associate Professor Arijit Raychowdhury. His research interest includes energy-efficient hardware design for distributed optimizations.



**Avinash L. Varna** (Member, IEEE) received the B.Tech. degree in electrical engineering from IIT Madras, Chennai, India, in 2005, and the Ph.D. degree in electrical engineering from the University of Maryland, College Park, MD, USA, in 2011.

He is currently a Principal Engineer with Intel Corporation, Chandler, AZ, USA. His research interests include the security of embedded systems, applied cryptography, information forensics, and multimedia security.

Dr. Varna served on the organizing committee of the IEEE International Workshop on Information Forensics and Security in 2014 and the IEEE Technical Committee on Information Forensics and Security from 2015 to 2017.



**Harish K. Krishnamurthy** (Senior Member, IEEE) received the Ph.D. degree in electrical engineering from Arizona State University, Tempe, AZ, USA, in 2008.

He is a Principal Engineer with Circuits Research Lab, Intel Labs, Hillsboro, OR, USA, working on power delivery circuits and systems. He has over 25 publications at leading IEEE conferences, over 20 issued patents, and over 30 patent applications filed to date. His research interests include topologies and digital control techniques for fully on-die switching power converters, fully synthesizable digital LDOs, and reconfigurable power delivery.

Dr. Krishnamurthy is currently serving as a Technical Program Committee Member for the Power management Sub-Committee at the International Solid-State Circuits Conference (ISSCC).

**Sanu Mathew** (Fellow, IEEE) received the B.Tech. degree in electronics and communications engineering from the College of Engineering, Trivandrum, India, in 1993, and the M.S. and Ph.D. degrees in electrical and computer engineering from the State University of New York at Buffalo, Buffalo, NY, USA, in 1996 and 1999, respectively.

He is currently a Senior Principal Engineer with Circuits Research Lab, Intel Corporation, Hillsboro, OR, USA, where he heads Security Arithmetic Circuits Research Group, responsible for developing energy-efficient computer arithmetic datapath circuits and special-purpose hardware accelerators for cryptography and security. He has been with Intel Corporation since 1999. He holds 110 issued/pending patents, has published 86 conference/journal articles, and authored two book chapters.

Dr. Mathew has received two Intel Achievement Awards for pioneering energy-efficient execution core integer datapaths circuit technologies and developing AES-NI hardware on Intel products. He also mentors Intel- and Semiconductor Research Corporation (SRC)-funded research projects in leading universities and has served on the program committees of the International Symposium on Computer Arithmetic (ARITH), the International Symposium on Low Power Electronics and Design (ISLPED), the Design Automation Conference (DAC), and the International System-on-Chip Conference (SOCC). He currently serves on the Technical Program Committee at the International Solid-State Circuits Committee (ISSCC).

**Santosh Ghosh** received the Ph.D. degree from IIT Kharagpur, Kharagpur, India, in 2011, from IIT Kharagpur, Kharagpur, India, in 2011, and completed his post-doctoral studies from COSIC, KU Leuven, Leuven, Belgium, in the area of cryptographic hardware and side-channel attacks.

In 2012, he joined Intel Corporation, Hillsboro, OR, USA, as a Security Researcher. He has coauthored about 58 research publications and 53 filed/issued U.S. patents. The primary focus of his research includes: 1) design and implement cryptographic hardware microarchitecture and RTL with the aggressive area, latency, and throughput constraints; multiple of them are already being deployed in high-volume Intel products; 2) investigate and develop timing, power, and EM side-channel countermeasures; and 3) collaborate with academic partners and provide cryptography and security guidance to Intel business units.

**Arijit Raychowdhury** (Senior Member, IEEE) received the B.E. degree in electrical and telecommunication engineering from Jadavpur University, Kolkata, India, in 2001, and the Ph.D. degree in electrical and computer engineering from Purdue University, West Lafayette, IN, USA, in 2007.

In January 2013, he joined the School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA, USA, where he is currently a Professor. From 2013 to July 2019, he was an Associate Professor and held the ON Semiconductor Junior Professorship in the department. His industry experience includes five years as a Staff Scientist in the Circuits Research Lab, Intel Corporation, Chandler, AZ, USA, and a year as an Analog Circuit Researcher with Texas Instruments Inc., Bangalore, India. He holds more than 25 U.S. and international patents and has published over 200 articles in journals and refereed conferences. His research interests include low-power digital and mixed-signal circuit design, design of power converters, sensors, and exploring interactions of circuits with device technologies.

Dr. Raychowdhury is the Winner of the Qualcomm Faculty Award in 2020, the IEEE/ACM Innovator under 40 Award, the NSF CISE Research Initiation Initiative Award (CRII) in 2015, the Intel Labs Technical Contribution Award in 2011, the Dimitris N. Chorafas Award for outstanding doctoral research in 2007, the Best Thesis Award, College of Engineering, Purdue University, in 2007, the SRC Technical Excellence Award in 2005, the Intel Foundation Fellowship in 2006, the NASA INAC Fellowship in 2004, and the Meissner Fellowship in 2002. He and his students have won several fellowships and 11 best paper awards over the years. He currently serves on the Technical Program Committees of the ISSCC, the VLSI Circuit Symposium, the CICC, and the DAC. He was an Associate Editor of the IEEE Transactions on Computer Aided Design from 2013 to 2018 and an Editor of the *Microelectronics Journal* (Elsevier Press) from 2013 to 2017.

**Shreyas Sen** (Senior Member, IEEE) received the Ph.D. degree in electrical and computer engineering from Georgia Tech, Atlanta, GA, USA, in 2011.

He is currently an Associate Professor in electrical and computer engineering with Purdue University, West Lafayette, IN, USA. He has over five years of industry research experience in Intel Labs, Qualcomm, and Rambus. He has coauthored two book chapters, over 135 journal and conference papers, and holds 14 patents granted/pending. His current research interests span mixed-signal circuits/systems and electromagnetics for the Internet of Things (IoT), biomedical, and security.

Dr. Sen was a recipient of the NSF CAREER Award 2020, the AFOSR Young Investigator Award 2016, the NSF CISE CRII Award 2017, the Google Faculty Research Award 2017, the Intel Labs Quality Award for industry-wide impact on USB-C type, the Intel Ph.D. Fellowship 2010, the IEEE Microwave Fellowship 2008, and seven best paper awards, including the IEEE CICC 2019 and the IEEE HOST 2017–2019. His work was chosen as one of the top-10 papers in the hardware security field over the past six years (TopPicks 2019). He is the inventor of the Electro-Quasistatic Human Body Communication, for which he was a recipient of the MIT Technology Review top-10 Indian Inventor Worldwide under 35 (MIT TR35 India) Award. His work has been covered by 100+ news releases worldwide, invited appearance on TEDx Indianapolis, the Indian National Television CNBC TV18 Young Turks Program, and NPR subsidiary Lakeshore Public Radio. He serves/has served as an Associate Editor for the IEEE DESIGN&TEST, an Executive Committee Member for the IEEE Central Indiana Section, and the Technical Program Committee Member of DAC, CICC, DATE, ISLPED, ICCAD, ITC, and VLSI Design, among others.