ASNI: Attenuated Signature Noise Injection for Low-Overhead Power Side-Channel Attack Immunity

Debayan Das, *Student Member, IEEE*, Shovan Maity, *Student Member, IEEE*, Saad Bin Nasir, *Member, IEEE*, Santosh Ghosh, Arijit Raychowdhury, and Shreyas Sen, *Senior Member, IEEE*

***Abstract*— Computationally-secure cryptographic algorithms implemented on a physical platform leak significant "*side-channel*" information through their power supplies. Correlational power attack is an efficient power side-channel attack (SCA) technique, which analyzes the statistical correlation between the estimated and the measured supply current traces to extract the secret key. The existing power SCA countermeasures are mainly based on reducing the SNR of the leaked information, power balancing, or gate-level masking, each of which introduces significant power, area or performance overheads, which calls for an efficient generic countermeasure. This paper presents ASNI: *Attenuated Signature Noise Injection*, which is an energy-efficient generic countermeasure, and shows SCA resistance on the AES-128 encryption as an application. ASNI uses a shunt low-drop-out (LDO) regulator to suppress the AES current signature by >200× in the supply current traces. The shunt LDO has been fabricated and validated in 130 nm CMOS technology. System-level implementation of the ASNI, with the AES-128 core operating at 40 MHz, shows that the system remains secure even after 1 M encryptions, with ∼ 25× reduction in power overhead compared to that of noise addition alone.**

***Index Terms*— Side channel attack (SCA), cryptographic hardware, power analysis attack, countermeasure, attenuated signature AES, shunt LDO, noise injection.**

I. Introduction

IN THE last few decades, strong cryptographic algorithms have been developed and extensively used in applications such as the Trusted Platform Module, as well as in various embedded devices like mobile phones and smart cards. Unfortunately, these mathematically-secure algorithms are implemented on a physical platform and these physical CMOS-based devices provide "side-channel" information in the form of power consumption [1], [2], electromagnetic emanations [3], [4], timing of encryption operations [5], [6], or acoustic vibrations [7]. These "side-channel" leakage information can be exploited by attackers to extract the secret key from an encryption device.

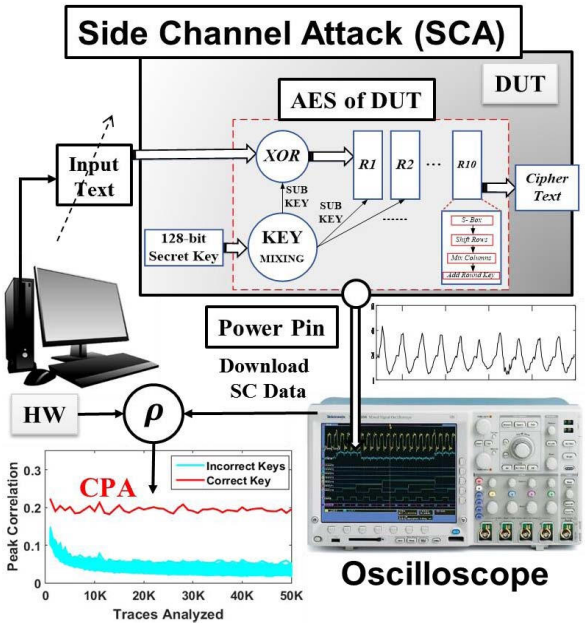


Fig. 1. Power Side-Channel attack on unprotected 128-bit AES.

A. Motivation

The power analysis attack (PAA) is one of the most common side-channel attacks on VLSI systems. These attacks are performed by measuring the power consumption of the encryption device under test (DUT). Subsequent simple (SPA) [8] or differential power analysis (DPA) [1] of the measured power traces reveals the secret key. Real-world examples of power SCA include the counterfeiting of e-cigarette batteries by stealing secret encryption keys from the authentic batteries to gain market share. In general, power analysis attacks can be used to extract the hidden key from the bootloader of any embedded VLSI device.

Figure 1 shows how a power side-channel attack (SCA) is performed. Initially, the power consumption of the device performing encryption is measured, and the power traces (T)

Manuscript received September 1, 2017; revised January 4, 2018 and February 18, 2018; accepted March 10, 2018. Date of publication April 27, 2018; date of current version August 30, 2018. This work was supported in part by the National Science Foundation (NSF) under Grant CNS 17-19235, Grant CNS 16-24810 (Center for Advanced Electronics through Machine Learning), and in part by Intel Corporation. This paper was recommended by Associate Editor R. Azarderakhsh. *(Corresponding author: Debayan Das.)*

D. Das, S. Maity, and S. Sen are with the School of Electrical and Computer Engineering, Purdue University, West Lafayette, IN 47907 USA (e-mail: das60@purdue.edu; maity@purdue.edu; shreyas@purdue.edu).

S. B. Nasir and A. Raychowdhury are with the School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA 30332 USA (e-mail: saadbinnasir@gatech.edu; arijit.raychowdhury@ece.gatech.edu).

S. Ghosh is with Intel Labs, Intel Corporation, Hillsboro, OR 97124 USA (e-mail: santosh.ghosh@intel.com).

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

Digital Object Identifier 10.1109/TCSI.2018.2819499

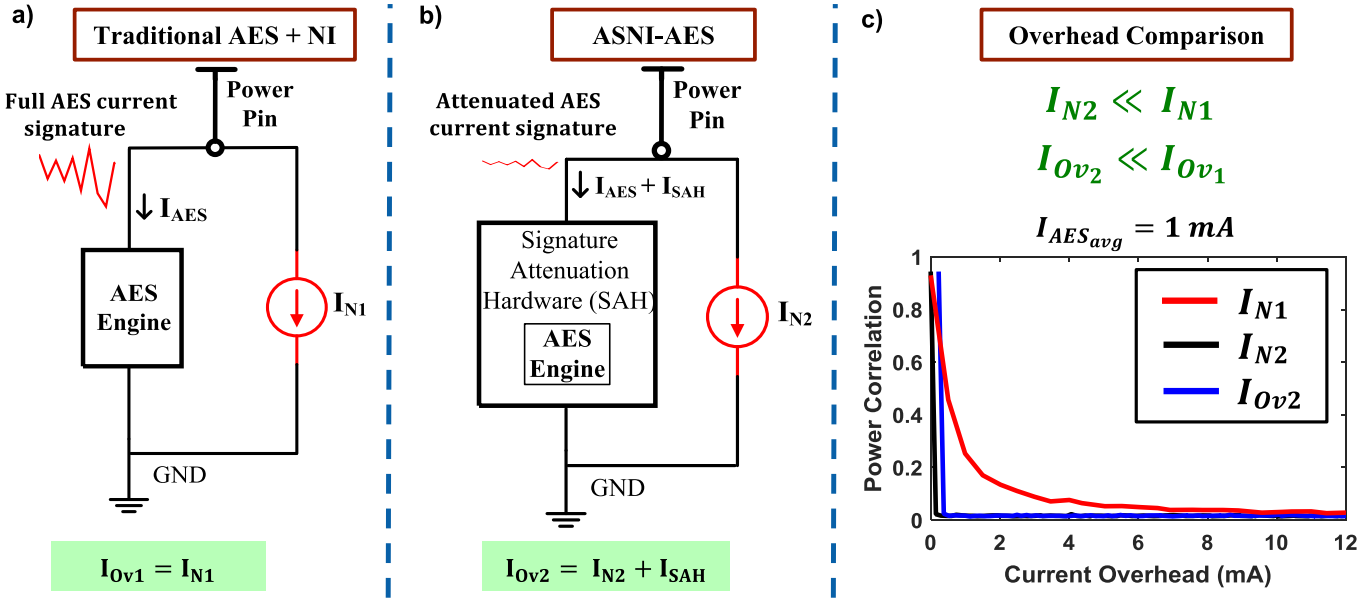


Fig. 2. (a) Traditional AES with Noise Injection, and (b) Proposed ASNI-AES, (c) Comparative Overview.

are collected over many different input plaintexts with the same secret key. Next, for a correlation power analysis (CPA) [9], a power model like the Hamming weight matrix (H) is built which contains the expected power consumption of the device performing a particular operation during encryption (like the S-Box substitution operation in the first round of AES), over the given plaintexts with all possible key bytes. This reduces the key search space of the AES-128 to $2^8 = 256$ possibilities for each key byte. Finally, the correlation coefficient (ρ_{TH}) between the power hypothesis (H) and the obtained traces (T) is calculated over time. One significant advantage of CPA is that the precise knowledge of the time instance when the targeted operation takes place during encryption is not required, as ρ_{TH} can be calculated at each sampling point of the trace. The key byte which shows the highest correlation represents the correct key byte. Repeating this process 16 times reveals the entire 128 bits of the secret key.

In this work, we focus on correlational power analysis (CPA) attack on a 128-bit Advanced Encryption Standard (AES) engine. The AES-128 engine under attack performs one block encryption in ten clock cycles. The S-boxes are implemented as lookup tables (LUTs) and are shared across rounds. It is to be noted that the proposed ASNI is a generic technique to resist power attacks, and can be applied to other encryption algorithms. The target of attack is the output of the S-Box operation in the 1st round [10]. Figure 2 gives an overview of the proposed ASNI-AES. Figure 2(a) shows the traditional AES with parallel noise incorporation to obfuscate the supply traces. The noise injection (NI) technique is discussed in Section IV. I_{ov1}, I_{ov2} denotes the total overhead currents for the traditional AES with NI alone and ASNI-AES respectively. The underlying idea of ASNI is to embed the encryption engine (AES) in a signature attenuating hardware (Figure 2(b)), such that the variations in the AES current is highly suppressed and is not reflected in the supply current traces, thereby requiring much lower noise current injection to decorrelate the measured supply traces (Figure 2(c)). A theoretical discussion on the analysis of overhead with reference to the Figure 2(c) is provided in Section III, IV.

B. Contribution

This paper proposes a new hardware-based countermeasure to resist power side-channel attacks. The main contributions of this article are summarized below.

- This work proposes ASNI as a generic *technique*, which involves Signature Attenuation followed by Noise Injection, leading to a low overhead countermeasure against power SCA. To achieve a Minimum Traces to Disclosure (MTD) > 50 K, ASNI-AES shows 1.23× power overhead over the traditional AES, compared to that of 17× in the case of only noise injection (NI) (Section III).
- This article presents the underlying *theory* behind our proposed Signature Attenuation Hardware (SAH) with Noise Injection. This generic power SCA countermeasure, achieved by embedding the encryption engine in a high efficiency SAH, suppresses the secret AES signature on the power pin. Injection of noise to mask SCA in the Attenuated Signature domain, reduces the noise injection overhead (∼170 μA) for SCA immunity by ∼100×, compared to standalone noise injection (Section IV, V).
- With the proposed ASNI, *experimental results* demonstrate that none of the secret key blocks of the AES-128 have been disclosed (MTD > *1 M*) with >25× lower power overhead compared to parallel noise incorporation (Section VII).
- A piecewise non-linear time-variant (PWNLTV) *model* is developed to better explain the small-signal (SS) to large-signal (LS) transient behavior of the ASNI circuit. Comparison with the system-level simulations shows a promising match, even with the variation of different design parameters (Section VI).

C. Paper Organization

The remainder of the paper is organized as follows. Section II summarizes the existing countermeasures against power SCA. In Section III, a commonly used countermeasure against power attacks in the form of noise addition is analyzed. Section IV discusses the theory behind the proposed ASNI architecture. In Section V, the design and operation of the ASNI circuit is discussed. Section VI provides a modelling of the shunt LDO based SAH. Section VII discusses the implementation results of the ASNI-AES. Section VIII concludes the paper.

II. Related Work

The existing hardware-based protection schemes for the encryption engines against power attacks can be classified into four prominent categories. The *first category* reduces side-channel leakage by equalizing the power consumption for the rising and falling edges of the clock. *Power balancing logic* implementations include the dual-rail circuits [11], [12], sense-amplifier based logic (SABL) [13], and wave dynamic differential logic (WDDL) [14]. The WDDL structure appears to be the first power attack resistant power-balancing circuit validated in silicon, with a *Minimum Traces to Disclosure* (MTD) of $\sim 21K$. However, the increased protection consumed $4\times$ power overhead, $3\times$ area, and a $4\times$ performance degradation.

The *second category* is *hardware masking*, in which each logic gate is replaced with a sophisticated one to achieve gate-level masking, leading to high area and power overheads [15], [16]. A false-key based masking technique combined with WDDL-based XOR gates for reconstruction, has been explored as a countermeasure in [17]. Although it presents a low overhead solution by using a fixed intermediate mask, the assumption that the AES implementation has a fixed key is not practical. In order to support dynamic keys, the implementation could be modified with a random mask, which will significantly increase the power and area overheads ($>2\times$). In addition, it is not a generic technique and cannot be directly extended to other cryptographic algorithms.

The next two categories are physical techniques – *noise injection* and *supply isolation*. Noise insertion suppresses the AES signature (reduces the SNR of the leaked information) by parallel noise injection [18]. However, solely noise addition is not an optimum technique to make a power attack infeasible. A statistical analysis for this technique is presented in Section III. Also, the effect of power delivery network (PDN) on SNR has been studied and a frequency-dependent noise injection circuit was implemented by Wang *et al.* [19].

The fourth category of protection reduces the power side-channel leakage information by isolating the supply from the encryption engine. It includes switched capacitor techniques [20]–[23] and integrated voltage regulator (IVR) based implementations [24]–[29]. The switched capacitor current equalizer module proposed by Tokunaga and Blaauw *et al.* [21], [22] demonstrated power SCA immunity, however, it resulted in a $2\times$ performance degradation on top of the 33% power overhead. Countermeasures based on random converter gating of multi-phase switched capacitor converter (SCC) have been presented in [30]–[33]. Depending on the workload requirements, phases are randomly reshuffled to obfuscate the current observed at the supply pin.

The impact of package parasitic and integrated buck converters on power SCA vulnerability have been analyzed in [19], and [24].

Another concept is to degrade the performance of IVR such that supply current has lesser correlation with the AES current. Implementations of this concept could be found using Analog LDO [25], Digital LDO (resolution is traded off, droop increases) [26] and a buck converter [27]–[29].

However, an ideal LDO-based implementation is inherently insecure. Traditional LDOs (Figure 3), which are commonplace in ICs, try to maintain a constant output voltage V_{reg}, which means $I_{sup} = I_{AES}$, and thus the supply current reflects

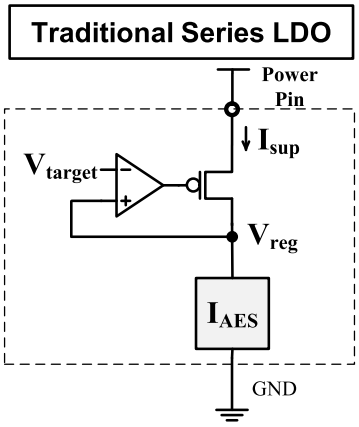


Fig. 3. Traditional Series LDOs, used as a countermeasure [26].

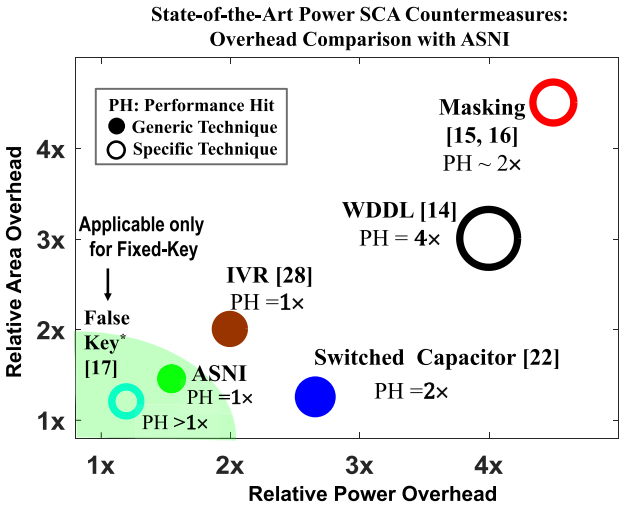


Fig. 4. Overhead comparison of the existing State-of-the-art hardware SCA countermeasures with ASNI. The area overhead ($1.6\times$) for ASNI is shown for $MTD > 1M$, while the area overhead is much less ($1.23\times$) for $MTD > 50K$ (Table 2). Size of each marker represents the relative performance degradation (PH). Generic techniques which can be directly applicable to other encryption engines are shown with filled markers. PH $= 1\times$ implies no performance degradation. *Only applicable for fixed-key AES implementations.

the changes in the load (AES) current. Hence, the above described LDO-based techniques introduce non-idealities in the system and thus, incur a fundamental trade-off between system performance (e.g. dynamic loop response) and reduction in side-channel vulnerability.

In this work, the proposed ASNI effectively combines the third and fourth categories of protection to achieve SCA immunity with high power efficiency and no performance degradation. Figure 4 summarizes the state-of-the-art related works, and shows the effectiveness of the proposed ASNI in terms of overhead, compared to the existing countermeasures [14], [16], [17], [22], [28], [29].

III. Efficacy of Noise Injection in Power SCA Immunity

Noise injection (NI) into power consumption measurements is a convenient approach to defend against power side-channel attacks [34]. The correlation (ρ_{TH}) between the estimated Hamming weight matrix (H) and the obtained power traces (T) can be given as,

$$\rho_{TH} = \frac{Cov\,(T, H)}{\sigma_T * \sigma_H} \tag{1}$$

where, Cov denotes the covariance matrix, and $\sigma_{T,}\sigma_H$, represents the standard deviation of T *and* H respectively. Now, the main goal is to add enough random noise to resist a side-channel attack, yet introducing a minimal power overhead in the system. If N_1 denotes the amount of random noise added into the circuit, and $T' = T + N_1$ denote the modified traces, the modified correlation factor $\rho_{T'H_{NI}}$ can be written as [35],

$$\begin{aligned}\rho_{T'H_{NI}} &= \frac{Cov\,(T + N_1, H)}{\sigma_{T+N_1} * \sigma_H} \\ &= \frac{E\,[(T + N_1) * H] - E\,(T + N_1)\,E\,(H)}{\sqrt{E\,(T + N_1)^2 - E^2\,(T + N_1)} * \sigma_H} \\ &= \frac{E\,[T * H] - E\,(T)\,E\,(H)}{\sqrt{E\,(T)^2 + E\,(N_1)^2 - E^2\,(T) - E^2\,(N_1)} * \sigma_H} \\ &= \frac{Cov\,(T, H)}{\sqrt{\sigma_T^2 + \sigma_{N_1}^2} * \sigma_H}\end{aligned} \tag{2}$$

E represents the expectation or mean of the corresponding variable. The independence of the variables N_1 and H has been utilized in this expression. Thus, we see from Eqn. 2 that, higher is its variance $\sigma_{N_1}^2$, lower is the correlation $\rho_{T'H_{NI}}$. However, noise insertion alone introduces a significant current overhead.

Figure 2(c) (red curve) shows the impact of only noise insertion on power SCA immunity. It can be clearly seen that for the actual key, the traces correlate in absence of noise ($\rho_{T'H_{NI}} \sim 0.9$). For the AES-128 core (40 MHz) under attack, the average current consumption of the sampled traces during the AES operations was found to be $\sim$*1 mA*. In order to provide high enough resistance to a DPA or CPA, noise insertion requires a current overhead of $\sim$17 mA (refer MTD plots in Figure 18(a-d)), which is approximately *seventeen times* (17×) of the average AES current consumption. Thus, only noise insertion is not an optimized solution for power SCA immunity.

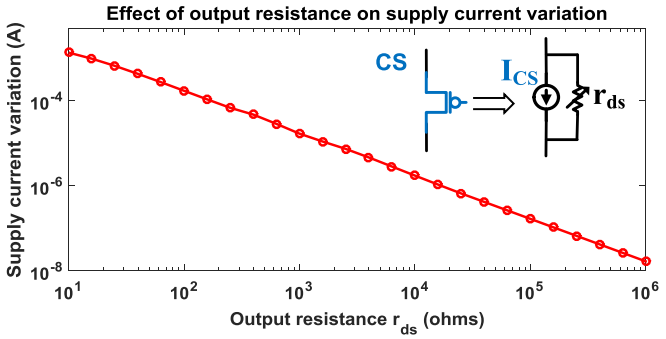


Fig. 5. Effect of output resistance of the current source on the supply current variation (Log-Log scale).

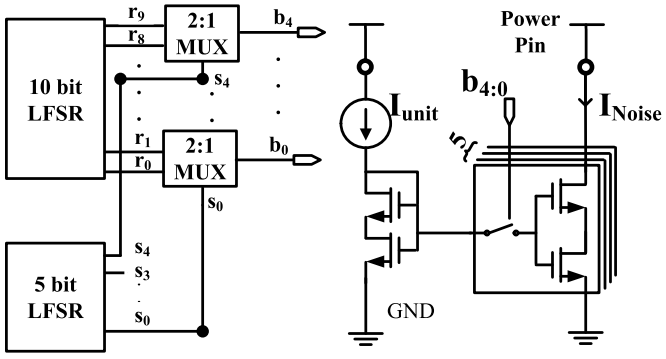


Fig. 6. Noise current generation circuit using 2-level stochastic 10-bit LFSR, followed by a 5-bit current steering DAC.

IV. ASNI – Theoretical Analysis

A. Signature Attenuation Hardware (SAH)

Now imagine, if we can somehow embed the AES engine in a Signature Attenuation Hardware (SAH) with an attenuation factor AF($\ll$1), then the noise current overhead required to decorrelate the traces is given by the modified correlational factor,

$$\rho_{T'H_{ASNI}} = \frac{(AF) * Cov\,(T, H)}{\sqrt{(AF)^2 * \sigma_T^2 + \sigma_{N_2}^2} * \sigma_H} \tag{3}$$

From Eqn. 3, it can be clearly seen that the noise variance ($\sigma_{N_2}^2$) required reduces by a factor of $\frac{1}{AF^2}(\gg 1)$, compared to only noise injection.

$$\sigma_{N_2}^2 = AF^2 * \sigma_{N_1}^2, \quad AF \ll 1$$

Hence the noise current overhead is reduced by a factor of $\frac{1}{AF}(\gg 1)$, as shown in Eqn. 4.

$$I_{N_2} = AF * I_{N_1}, \quad AF \ll 1 \tag{4}$$

As long as the SAH power consumption is low enough, the current overhead (I_{Ov_2}) for ASNI would be reduced significantly.

$$I_{Ov_2} \sim AF * I_{Ov_1}, \quad AF \ll 1$$

Figure 2(c) (blue curve) shows the significant improvement ($\sim$100×) in the noise current overhead for ASNI ($\sim$170 μA, refer MTD plots in Figure 18), compared to only noise insertion.

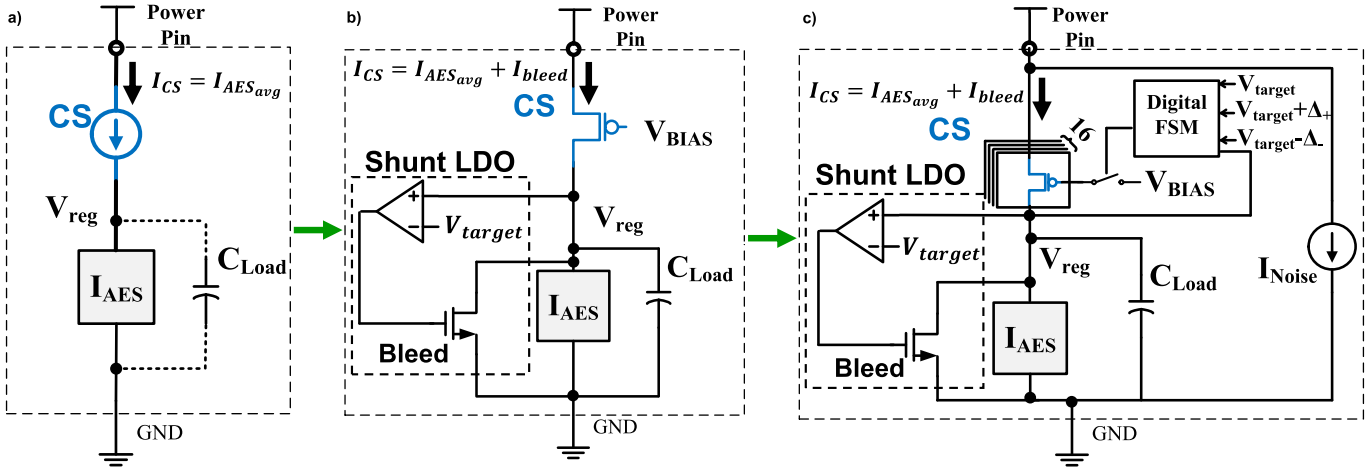


Fig. 7. Build-up to the SAH: (a) An ideal implementation, (b) SAH with the analog shunt LDO loop with voltage regulation, (c) Proposed ASNI-AES architecture with noise injection to defend against power side-channel attacks (FSM refers to Finite State Machine of the digital SMC loop).

Ideally, it is desirable to design a SAH such that the AES signature is fully suppressed, and the supply current becomes independent of the AES current, that is,

$$Attenuation = \frac{1}{AF} = \infty \tag{5}$$

B. Noise Injection (NI)

Hardware implementation of an AES engine is driven by a current source (CS). An ideal CS has an infinite output resistance, and hence does not reflect any load variations. However, in physical devices, a biased PMOS is used as the current source, which suffers from a finite output resistance.

Figure 5 shows the peak-to-peak supply current variation with change in the output resistance (r_{ds}) of the CS. Even designing a current source with output resistance in the order of MΩ (cascode stage) would reflect a variation in the order of nA, which can still be measured using an oscilloscope. Thus, a change in AES current in the order of mA gets reflected in the supply current in an attenuated scale of the order of few μA, depending on the impedance of the current source.

Hence, even after attenuating the AES signature using the SAH, the change in AES load current still reflects in the power supply traces, and does not resist a CPA attack completely, resulting in some correlational peaks. Thus, a small amount of random noise current is injected (as shown in Figure 6, Figure 7(c), and also discussed in Section V) in order to decorrelate the traces with the estimated Hamming weight matrix, and thereby provide significant immunity against CPA attack. The noise injection (NI) circuit involves a 2-level stochastic linear feedback shift register (LFSR) stage followed by a 5-bit current steering Digital to Analog Converter (DAC). A 5-bit LFSR is used to stochastically sub-sample the 10-bit LFSR to produce a 5-bit output. 5 binary-weighted NMOS current sources are turned on or off depending on the LFSR output ($b_{4:0}$) to obfuscate the current traces obtained from the power pin. The use of an additional 5-bit LFSR is done to sub-sample the 10-bit output stochastically, thereby reducing the area overhead of the binary-weighted current DAC (5-bit instead of 10-bit), while maintaining the period of $2^{10} - 1 = 1023$. The stacking of transistors improves the linearity of the NI circuit, as the bottom transistor in linear region acts as a source degenerate for the upper transistor. Noise overhead for ASNI is very minimal compared to the noise injection (NI) technique alone and depends on the output resistance of the driving current source PMOS, and small-signal variation present in the output node. Thus, the total current overhead for ASNI includes the current consumed by the SAH and the noise overhead.

V. Design of the Signature Attenuation Hardware

In this section, we introduce the proposed signature attenuation hardware (SAH). Our goal is to develop a SAH such that the supply current (I_{CS}) is highly independent of the AES transitions (high attenuation: $AF \rightarrow 0$), without any performance degradation.

A. Design Flow: Build-Up to the Proposed SAH

The first thing that comes to mind is a constant current source. However, a constant current source cannot drive a variable current load (AES). Hence, we need an additional element, or a capacitor to account for the difference in current, as shown in Figure 7(a). This ideal topology works, but with a high fluctuation at the output node (V_{reg}), leading to a performance hit.

Now, as shown in Figure 7(b), we introduce a control loop, which senses the output voltage V_{reg}, and controls the bleed NMOS gate voltage to draw any instantaneous excess current from the supply, thereby restricting any unnecessary charging of the load capacitor. This topology, called the shunt LDO-based loop is able to simultaneously regulate V_{reg}, while maintaining the supply current (I_{CS}) independent of the AES transitions (I_{AES}). The biased PMOS on top acts as a constant current source. To compensate for process, frequency, and temperature variations, a slow digital loop with switched mode control is incorporated, as shown in Figure 7(c).

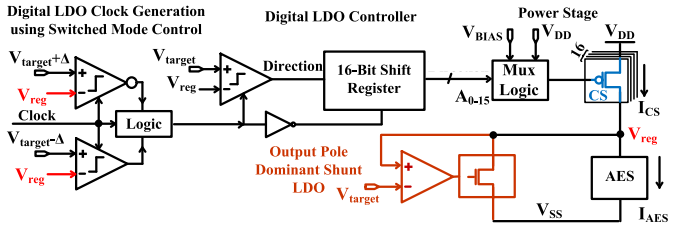


Fig. 8. Block diagram of the SMC loop with shunt LDO.

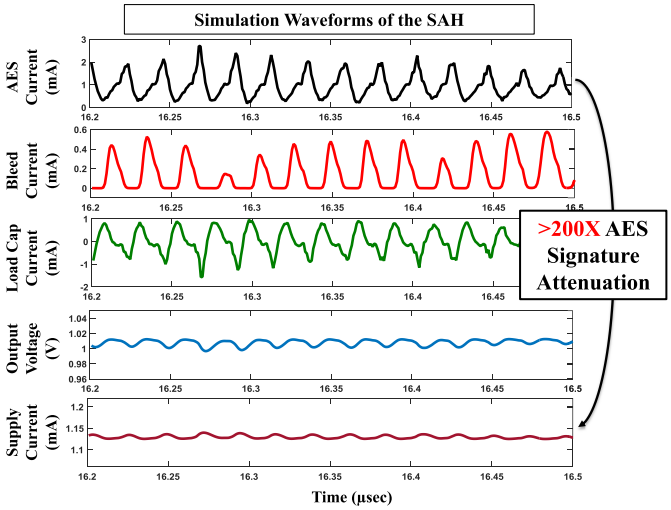


Fig. 9. Snapshot of the time-domain waveforms of the SAH.

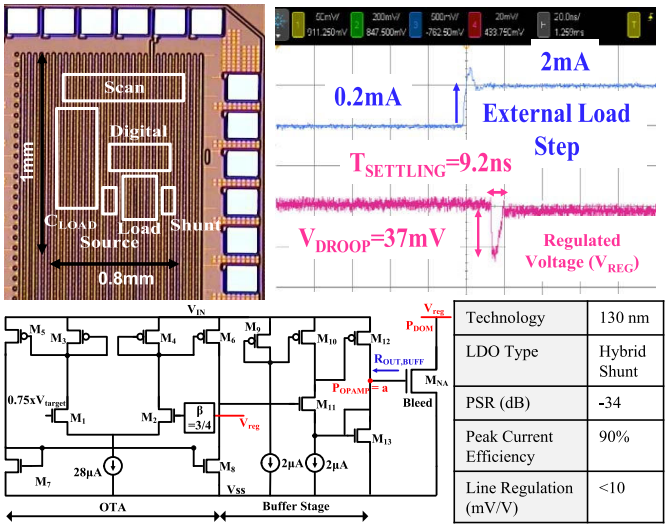


Fig. 10. Proof-of-concept shunt LDO design measured on a 130 nm testchip. Die-photo, key measurement results and the shunt LDO circuit is shown.

B. Operation Principle of the SAH

The proposed SAH operates using two control loops (Figure 7(c)). Switched-mode control (SMC) is implemented using a low bandwidth slow loop to track large changes in the average AES current. The concept of SMC is demonstrated in [36].

The SMC loop (Figure 8) regulates the current through an array of PMOS current sources, which are activated when the output voltage goes beyond $V_{target} \pm \Delta$. Here Δ acts as a guard-band and prevents the digitally controlled loop from being continuously ON. As V_{reg} becomes $< V_{target} - \Delta$, or $> V_{target} + \Delta$, the detection stage comparators un-gate the clock to turn on the following clocked comparator. Now, if $V_{reg} < V_{target}$, (or $V_{reg} > V_{target}$) the shift register passes '0' (or '1' respectively) to turn on (or off) a PMOS transistor. As soon as the output voltage is within Δ, the digital loop is gated and the analog shunt regulator takes the output voltage to V_{reg}. For the AES-core under attack, it was verified that the average current ($\sim 1\ mA$, in this case) consumed by the AES engine for different inputs remain almost the same throughout the encryption operations, as it performs repetitive ten round operations for each input block. SMC only engages to compensate for slow changes in the average AES current. Due to the almost-constant nature of the average AES current, the SMC loop stays disengaged and the PMOS (Figure 7(c)) acts as a current source (CS), in saturation, with high drain to source impedance (r_{ds}).

Once the SMC loop is set, the CS current is fixed at a value higher ($I_{CS} = I_{AES_{avg}} + I_{bleed}$) than the average load (AES current). The fast loop incorporates a shunt LDO with a NMOS bleed to sink any excess current from the supply, when the AES current consumption is lower than the supply current (I_{CS}). Thus, the bleed restricts unnecessary charging of the load capacitor (C_{Load}), and thereby regulates the output voltage (V_{reg}). On the other hand, when the AES current requirement is more than the supply current, the capacitor provides the necessary extra current, thereby maintaining a constant supply current irrespective of the AES current variation, at the expense of an instantaneous droop in V_{reg}, which is reduced with increased C_{Load} or I_{bleed}.

Figure 9 shows the time-domain waveforms of the ASNI-AES during an encryption operation. It can be seen that when the AES current goes low, the bleed sinks the excess current, not allowing the load capacitor to charge up, and thereby maintaining a constant V_{reg}. Output voltage (V_{reg}) with low ripples ensure that the AES current variation is sufficiently suppressed in the supply current. When the bleed device turns off, the load capacitor delivers the required current, thereby maintaining the supply current at a constant value, however causing a small droop. In Figure 9, an average droop of $\sim 10\ mV$ in V_{reg} can be observed whenever the AES current shows a rising spike, using a 450 pF integrating capacitor (C_{Load}). High output resistance (r_{ds}) of the PMOS minimizes supply current variations caused by the signature of the small V_{reg} variations. Since an ideal constant current source (as discussed in Section IV) is not feasible, a finite r_{ds} would still reflect the relative change in voltage V_{reg} in the supply current, however, it will be highly attenuated ($>200\times$). Hence, a tiny amount of random noise current is injected (as shown in Figure 7(c)) to decorrelate the supply traces with the estimated HW matrix, thereby providing a significant immunity against CPA attack. The amount of noise injection required, as well as the total current overhead for ASNI is quantitatively analyzed in Section VII.

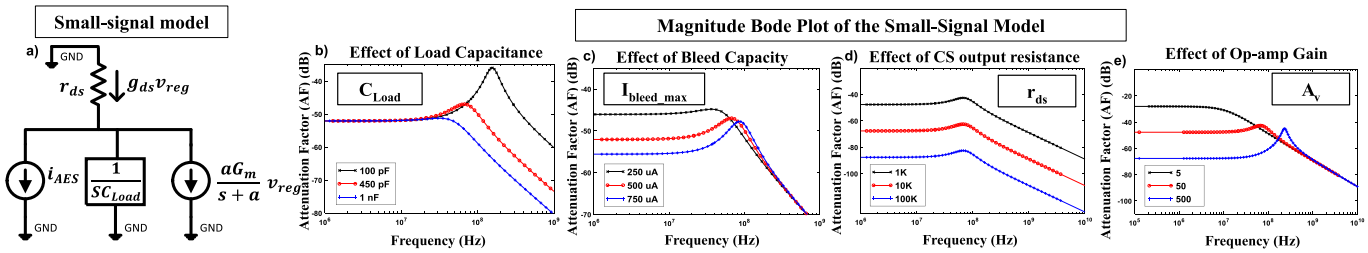


Fig. 11. (a) Small-signal model of the SAH, (b-e) Effect of design parameters on the magnitude Bode plot for attenuation factor (AF) of the Signature Attenuation Hardware (SAH) - (b) Load capacitance, (c) Bleed capacity, (d) CS output resistance, (e) op-amp gain.

C. Validation of the SMC-Based Shunt LDO

The feasibility of a linear regulator featuring SMC and shunt regulation has been shown in Figure 10. A proof-of-concept design has been fabricated in the 130 nm CMOS technology. In the chip micrograph, Shunt refers to the analog shunt LDO, Digital refers to the digital SMC block, and C_{Load} is the output load capacitance.

The digital control loop allows large signal control of the input current and is activated when the output voltage goes beyond $V_{target} \pm \Delta$. The shunt analog regulator is a two stage design with an operational transconductance amplifier (OTA) based first stage and a shunt feedback buffer based second stage. It is designed to be output pole dominant (OPD) in order to provide high gain and bandwidth for small-signal regulation. The first stage of the OPD analog LDO comprises of a self-biased transconductance (g_m) stage that uses a differential pair with diode connected load transistors. The second stage comprises of a shunt buffer to push the pole at the gate of the bleed transistor (P_{OPAMP}) to a higher frequency, thereby making the LDO output pole (at node V_{reg}) dominant. Note that the dominant pole of the op-amp is P_{OPAMP}, while the dominant pole of the shunt LDO is P_{DOM} at the output. $\beta = \frac{3}{4}$ downscales the output voltage (V_{reg}) to meet the ICMR (Input Common Mode Range) of the op-amp. In the current test-chip, $\Delta = 70$mV has been chosen. The shunt (bleed) path is designed to consume 5% to 40% of the load (AES) current and provide regulation. A scope capture of fast transient response to a load step shows a settling time of 9.2 ns, and a worst-case voltage droop of 37 mV. The phase margin in the worst case load condition is 88° . A summary of the measurements on the test-chip is also shown. Peak current efficiency of 90% is measured. This measured line regulation is less than 10 mV/V. This design illustrates the concept of an SMC based shunt LDO and the capability of the design to provide regulation across a load range.

VI. Modelling of SAH

In its steady state, the proposed Signature Attenuation Hardware (SAH) switches between small-signal (SS) and large-signal (LS) domains. As long as the instantaneous AES current (i_{AES}) remains lower than the supply current (I_{CS}), the circuit exhibits small-signal behavior, and the fast shunt LDO loop remains engaged. However as the instantaneous load current i_{AES} goes higher than the supply I_{CS}, the circuit switches to the large-signal domain, the bleed NMOS turns off, and the instantaneous excess current is provided by the load capacitor.

A. Small-Signal (SS) Analysis of the SAH

The parameters involved in the design of the fast control loop of the SAH are the NMOS bleed size, the choice of integrating load capacitor, gain (A_v) and bandwidth of the operational amplifier (op-amp) in the shunt LDO loop (Figure 7(c)). When $i_{AES} < I_{CS}$, and the transistors are properly biased into saturation and considering steady state operation, the small-signal analysis of the SAH can be performed (Figure 11(a)). The small-signal analysis is shown as follows:

$$-g_{ds}v_{reg} = i_{AES} + v_{reg}SC_{Load} + \frac{aG_m}{S+a}v_{reg}; \quad G_m = A_v g_m.$$

$$\frac{v_{reg}}{i_{AES}} = -\frac{1}{g_{ds} + SC_{Load} + \frac{aG_m}{S+a}}$$

$$\frac{i_{CS}}{i_{AES}} = \frac{g_{ds}}{g_{ds} + SC_{Load} + \frac{aG_m}{S+a}}$$

$$AF_{SS} = \frac{g_{ds}}{C_{Load}} \times \frac{s+a}{\left[S^2 + S\left(a + {}^{g_{ds}}/_{C_{Load}}\right) + (aG_m + ag_{ds})/C_{Load}\right]} \tag{6}$$

where, AF is the AES signature attenuation factor; g_m is the transconductance of the NMOS bleed; A_V and a represents the dc gain and the dominant pole of the op-amp respectively.

Figure 11(b-e) shows the effect of parameters on the attenuation factor (AF) over frequency. Figure 11(b) shows the effect of load capacitance (C_{Load}) variation on AF. As the load capacitor is increased, attenuation ($\frac{1}{AF}$) increases. $C_{Load} = 100\ pF$ shows a prominent peak due to the output pole of the op-amp (a), which in turn contributes a 'zero' for the system, reducing the attenuation. Note that $a = P_{OPAMP}$ (Figure 10). However, as C_{Load} is increased, attenuation increases, as the shunt LDO SAH enters the output-pole dominant region. Figure 11(c) shows that as the bleed capacity is increased, AF reduces, that is, attenuation increases. Higher output resistance (r_{ds}) of the CS provides more attenuation, as shown in Figure 11(d). Higher gain (A_V) of the op-amp reduces the delay for the bleed to turn on, and thus attenuation increases, as seen from Figure 11(e). It is to be noted that very high A_V will increase the Miller capacitance C_{gd}, which will

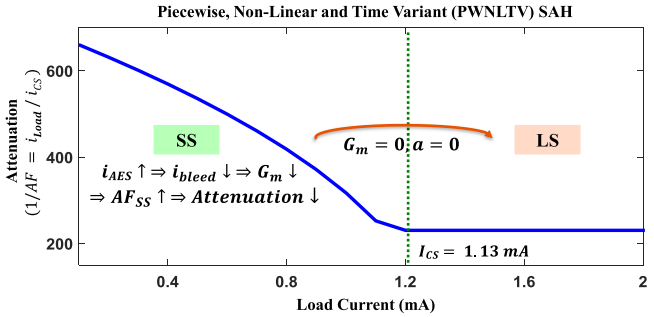


Fig. 12. Piecewise, non-linear and time variant behaviour of the SAH.

TABLE I
NOMINAL PARAMETERS USED IN THE SAH DESIGN

Parameters	Nominal Values
Load Capacitor (C_{Load})	450 pF
Op-amp Gain (A_v)	50
Bleed Capacity ($i_{bleed_{max}}$)	700 μA
Clock Frequency ($\omega/2\pi$)	40 MHz
Dominant Pole of op-amp (a)	~400 MHz

reduce the dominant pole (a) of the op-amp, thus lowering the bandwidth of the loop. Table 1 shows the nominal parameters used for the SAH design.

B. Large-Signal (LS) Analysis of the SAH

As the load AES current exceeds the supply current ($i_{AES} > I_{CS}$), the shunt LDO loop is disengaged and the circuit switches to large-signal domain. The large-signal attenuation is given as:

$$-g_{ds}v_{reg} = i_{AES} + v_{reg}SC_{Load}$$
$$AF_{LS} = \frac{i_{CS}}{i_{AES}} = \frac{g_{ds}}{g_{ds} + SC_{Load}} \quad (7)$$

Note that the Eqn. 7 can be derived from the expression $|AF_{SS}|$ (Eqn. 6) by setting $g_m = 0, a = 0$ (Figure 12).

Ideally, if the integrating capacitor (C_{Load}) is high enough, so as to deliver any excess current drawn by the AES, and if the bleed transistor is strong enough to sink any extra current (continuous small-signal operation), and the shunt LDO loop bandwidth is very high, then $AF \approx 0$ and the droop in the output voltage V_{reg} would be negligible. However, continuous small-signal operation requires more overhead current and thus has a direct trade-off with the power efficiency. Also, bandwidth of the fast loop is limited due to the presence of a pole at the gate of the bleed NMOS. Also, the choice of capacitor has a trade-off with the area. The choices of the optimized design parameters (Table 1) are further elucidated in Section VII.

C. SS-LS Transition: PWNLTV Model

The proposed SAH can be modelled as a piecewise, non-linear, time variant ($PWNLTV$) system, as it switches from small-signal (SS) to the large-signal (LS) domain dynamically

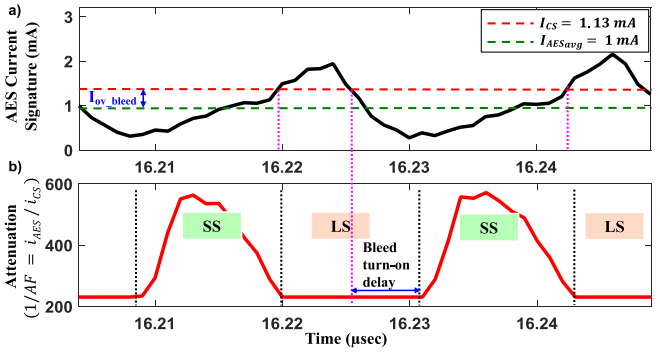


Fig. 13. SS-LS Transitions: (a) AES Current signature, (b) Attenuation due to the SAH in time domain, for this AES signature.

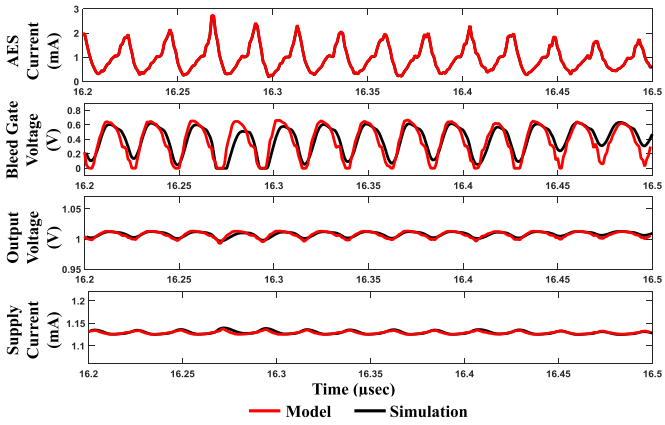


Fig. 14. SAH: Model & Simulation Comparison.

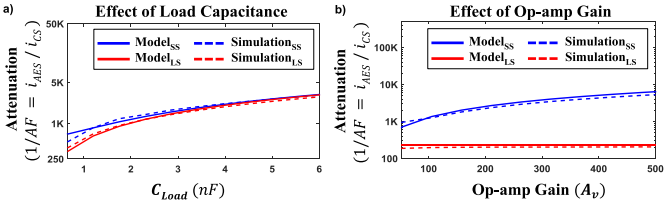


Fig. 15. Model vs. Simulation - Effect of design parameters on Small-signal (SS) & Large-signal (LS) AF: (a) Load capacitance, (b) Op-amp gain.

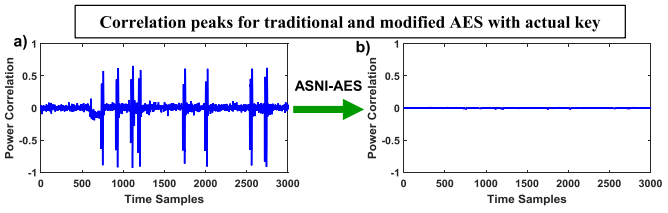


Fig. 16. (a, b): CPA attack on traditional and modified AES (with noise addition) respectively, for the actual key.

with the change in the load current, as shown in Figure 12. In this work, the load is the AES encryption engine. It should be noted that ASNI is a generic countermeasure, and can be applicable for other encryption engines as well.

As the AES current (i_{AES}) increases, the SS attenuation reduces and as $i_{AES} > I_{CS}$, SAH enters the LS region, where

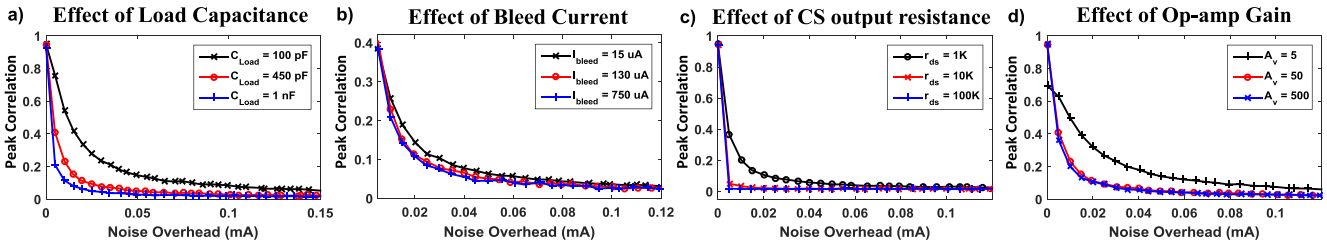


Fig. 17. (a-d): Effect of design parameters on the noise current overhead required for reducing the peak power correlation for the correct key byte to achieve high power attack immunity. (a) Load capacitance; (b) Bleed current sink capacity; (c) PMOS current source output resistance (r_{ds}); (d) Op-amp gain (A_V).

the attenuation becomes independent of the AES current. Hence, AF changes non-linearly with time, as shown in Figure 13(a, b). The attenuation factor for the PWNLTV model during the steady state operation of the SAH (SMC loop disengaged) is expressed as follows:

$$AF = AF_{SS}, \quad if\ i_{AES}(t) < I_{CS}\ \&\ A_v * \left(V_{reg} - V_{target}\right) > V_{Tn}$$
$$= AF_{LS}, \quad otherwise. \tag{8}$$

The model also takes into account the time lag in V_{reg} for the AES load, due to the capacitor. During the LS to SS transitions, further delay is caused to turn on the NMOS bleed, as seen from Figure 13(b), and has been taken in consideration in Eqn. 8. The bleed turn-on delay reduces as C_{Load} is increased, and thus SAH stays in SS region showing higher attenuation, but at the expense of more area. Figure 14 shows a strong match between the modelled SAH time-domain waveforms with the system-level simulation. Figure 15 shows the contrast between the SS and LS attenuation with variation in the load capacitance (C_{Load}) and the op-amp gain (A_v). For lower values of the C_{Load}, SS attenuation dominates the LS. However, as C_{Load} is increased, V_{reg} droop reduces, and SS attenuation approaches the LS attenuation, as shown in Figure 15(a), and is also evident from Eqns. 6, 7. Increasing the op-amp gain (A_v) increases the SS attenuation, but does not impact the LS attenuation, as seen from Figure 15(b). Figure 15 also shows a promising match of the model results and the simulations with the variation of parameters.

The choice of the optimal design parameters for ASNI and the resulting overheads are discussed quantitatively in the next section.

VII. Results

A. CPA Attack on the AES-128 Core

We perform CPA attack on the AES-128 core with clock frequency of 40 MHz and an average current ($I_{AES_{avg}}$) of ~1 mA (peak current = 3.2 mA). Figure 16(a) shows the correlational peaks for the actual key when the unprotected AES was subjected to CPA attack ($< 1K$ traces). The same attack on ASNI-AES does not reveal the secret key, highlighting the SCA immunity (Figure 16(b)).

B. Design Space Exploration

Figure 17(a-d) shows the effect of design parameters on the noise current overhead, that is required to decorrelate the traces for the actual key. Figure 17(a) shows that with the increase of C_{Load}, the noise overhead (I_{noise}) reduces. However, there is a trade-off between the area and the current/power overhead. For $C_{Load} = 100\ pF$, the V_{reg} droop is higher, leading to performance degradation. Hence, $C_{Load} = 450\ pF$ is an optimal design choice. Figure 17(b) shows that an average bleed current (I_{bleed}) of ~130 μA is an optimal choice. A larger bleed current implies higher I_{CS}, but does not necessarily reduce the required noise overhead in spite of a high SS attenuation, as some of the correlation spikes show up during the LS operation of the ASNI-AES. However, a lower choice of bleed overhead will result in V_{reg} variations, due to the unnecessary charging of the load capacitor. It is to be noted that although the average $I_{bleed} = 130\ \mu A$ (set by the I_{CS}), the peak current through the bleed (bleed capacity) is ~700 μA. Hence, $I_{CS} = I_{AES_{avg}} + I_{bleed} = 1.13\ mA$, and the bleed is optimally designed to have a current sink capacity of 700 μA.

Figure 17(c) shows that the higher output resistance ($r_{ds} = 100\ K\Omega$) of the PMOS current source allows lower noise current overhead and thus the total overhead current is reduced. Figure 17(d) shows that op-amp gain (A_V) ~ 50 is an optimal choice, as higher A_V does not provide any benefit in reducing the current overhead, but can reduce the bandwidth of the shunt LDO loop, as discussed earlier.

The above results were obtained with $50K$ traces, and gives a good sense of the choice of design parameters and its effects.

C. SCA Immunity Verification With MTD Analysis

To confirm the exact overheads and efficiency, MTD analysis has been performed for $50K$ traces. As the number of traces analyzed is increased, the correlation coefficients (ρ) are expected to be more accurate, and ρ for the correct key should be consistently higher than the ρ of the peak (absolute maximum) correlation of the incorrect keys.

Figure 18(a-d) (noise addition alone) and Figure 18(e-h) (ASNI-AES) shows the change in correlation coefficient with the number of traces analyzed for different noise current injection. Figure 18(a-d) shows that only noise injection involves an overhead of 17 mA to achieve Measurements to Disclosure (MTD) > $50K$. As the ASNI-AES core is subjected to a CPA attack, it is seen that MTD > $50K$ is achieved with a noise current injection of only 170μA (Figure 18(h)). Also, the current consumed by the op-amp is ~100 μA. Hence, the

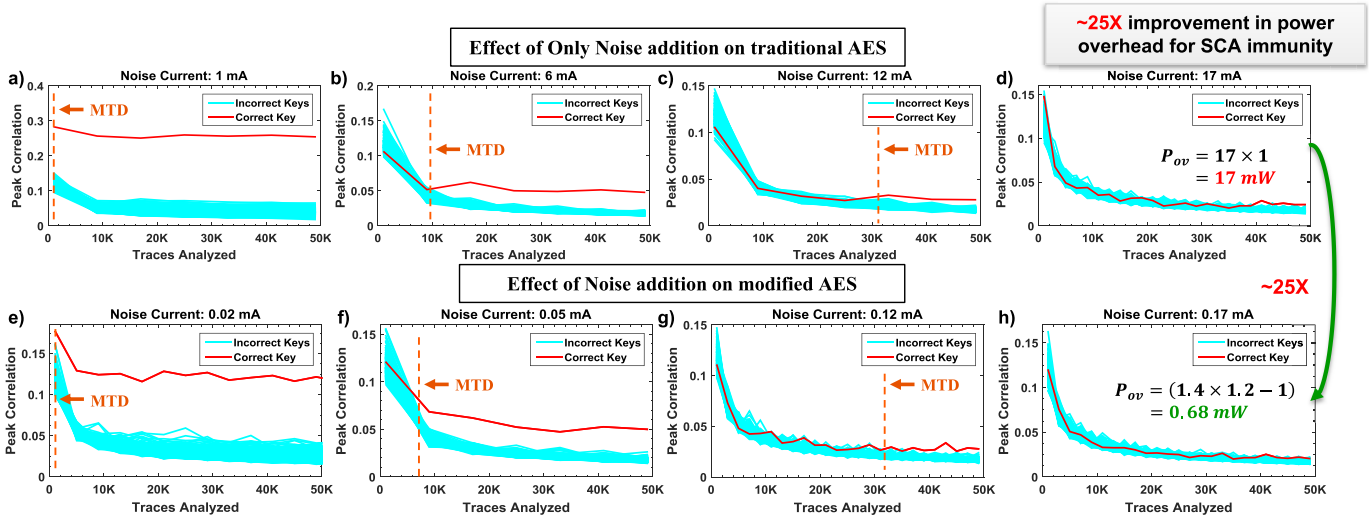


Fig. 18. (a-d): MTD plots for only noise addition on traditional AES; (e-h): MTD plots for noise injection on the modified AES (ASNI-AES).

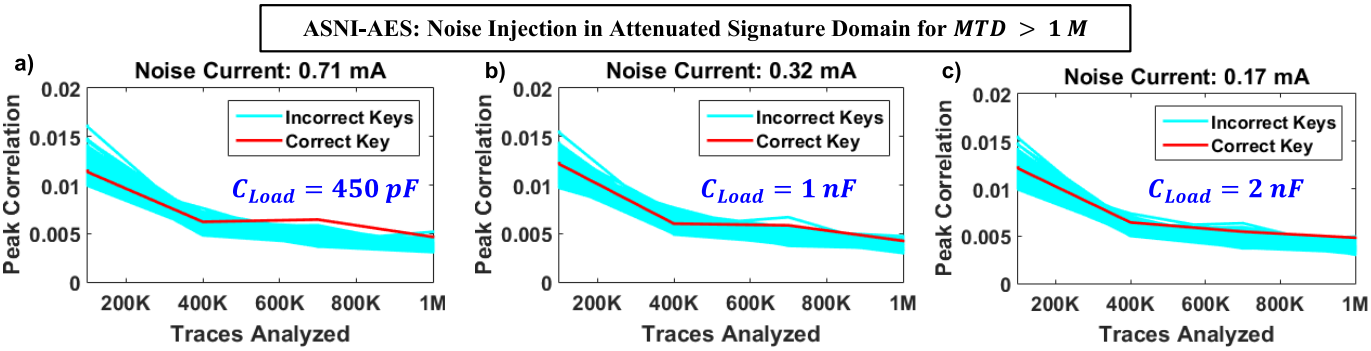


Fig. 19. (a-c): Noise Injection on the modified AES in Attenuated Signature domain to achieve MTD of 1 Million traces. Power efficiency vs. area overhead trade-offs can be observed.

total overhead current is given as,

$$I_{ov} = I_{bleed} + I_{noise} + I_{opamp} = 130\,\mu A + 170\,\mu A + 100\,\mu A = 0.4\,mA,$$

which is $>40\times$ lower than that of noise addition alone. Note that the unprotected traditional AES block operates at a supply voltage of 1 V. Introduction of the SAH increases the supply to 1.2 V, while maintaining the same voltage across the protected AES ($V_{reg} = 1\,V$). The total overhead power for the ASNI-AES architecture is given as $(1.13\,mA + 0.17\,mA + 0.1\,mA) * 1.2\,V - 1\,mA * 1\,V = 0.68\,mW$, which translates to power overhead $P_{ov} = \frac{1.4\,mA * 1.2\,V}{1\,mA * 1\,V} * 100 \approx 68\%$, compared to the traditional unprotected AES. In case of solely noise insertion the power overhead required is $P_{ov} = 17\,mA * 1\,V = 17\,mW$. Thus, the SAH along with noise injection provides $\sim 25\times$ improvement in the power overhead for iso-SCA immunity, compared to only noise addition, with $MTD > 50K$.

Figure 19(a-c) shows the noise current overhead vs. area (C_{Load}) trade-off to achieve a $MTD > 1M$. To maintain the power efficiency of $\sim 60\%$, a larger load capacitor $C_{Load} = 2\,nF$ is required, which translates to an area overhead of $\sim 1.6\times$. It should be noted that considering the presence of a shunt LDO in the system for voltage regulation makes the area overhead of ASNI negligible. However, the analysis of overhead has been performed without any such assumptions.

D. Comparison With the State-of-the-Art Hardware Protection Schemes

Power efficiency for ASNI-AES is given as, $\eta = \frac{1}{1+P_{ov}} * 100 = \frac{1}{1.68} \approx 60\%$ (includes noise overhead). Hence, ASNI-AES consumes similar overhead as [21], but does not incur the performance penalty. Implementation of the SAH in 130 nm technology consumes an area of $\sim 0.08\ mm^2$, while a standalone AES incurs 0.35 mm^2, which implies an area overhead of $\sim 22.85\%$ in order to achieve $MTD > 50K$ ($\sim 60\%$ for $MTD > 1M$). A comparative analysis of overhead of ASNI with the prominent state-of-the-art hardware countermeasures [14], [16], [17], [22], [28], [29], [32] against power SCA is shown in Table 2. It highlights the advantages of using ASNI with low overheads and high power efficiency compared to the existing countermeasures (Figure 4).

VIII. Conclusion

Power Side Channel Attack is a prominent attack on cryptographic ICs. This work proposes low-overhead hardware modification that attenuates critical AES signature by $>200\times$ in the supply current which the attackers could

TABLE II
OVERHEAD COMPARISON OF ASNI-AES AGAINST THE EXISTING POWER SCA COUNTERMEASURES

Parameters	This Work	ISSCC '09 [22]	JSSC '06 [14]	TCAS-1 '16 [32]	TCAS-1 '17 [17]	ISSCC '17 [28]	CHES '07 [16]
Technology	130 nm	130 nm	180 nm	130 nm	130 nm	130 nm	130nm
Technique Used	ASNI	Switched Capacitor	WDDL	Converter Reshuffling (CoRe)	False key + selective WDDL **	IVR	Masking (MDPL)
Power	1.68×	2.66×	4×	–	∼1×	– 1.6× (60mA load) * > 2× (10mA load) *	– Very High
Area	∼1.23× (MTD = 50K) ∼1.6× (MTD=1M)	1.25×	3×	–	∼1.03×	– ∼2× *	4×
Performance Degradation	0	2×	4×	–	∼1.02×	0	∼2×
MTD	$> 1\ M$ (1000×)	$> 10\ M$ (2500×)	∼255K (30×)	> 9100×	$> 30\ M$ (187.5×)	$> 100\ K$ (100×)	–

– Not Reported; * Estimated from [28], [29]; **only applicable to fixed-key AES implementations (not a practical assumption).

observe from the periphery of an encryption ASIC. Noise injection in the attenuated signature domain achieves SCA immunity with extremely high energy-efficiency. Successful SCA immunity is demonstrated for a CPA side-channel attack, with over $1M$ traces. Power SCA immunity is achieved with 1.6× area overhead, 60% power efficiency compared to the unprotected AES engine, and 25× lower power overhead compared to only noise addition and more importantly without imposing any performance penalty. Finally, the proposed ASNI is a generic power SCA countermeasure and can be extended to other cryptographic engines.

REFERENCES

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

[2] E. Brier, C. Clavier, and F. Olivier, "Optimal statistical power analysis," Cryptol. ePrint Arch., Tech Rep. 2003/152, 2003. [Online]. Available: https://eprint.iacr.org/2003/152

[3] J.-J. Quisquater and D. Samyde, "ElectroMagnetic Analysis (EMA): Measures and Counter-measures for Smart Cards," in *Smart Card Programming and Security*. Berlin, Germany: Springer, 2001, pp. 200–210.

[4] K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic analysis: Concrete results," in *Cryptographic Hardware and Embedded Systems—CHES*. Berlin, Germany: Springer, 2001, pp. 251–261.

[5] P. C. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems," in *Advances in Cryptology—CRYPTO*, N. Koblitz, Ed. Berlin, Germany: Springer, 1996, pp. 104–113.

[6] D. Brumley and D. Boneh, "Remote timing attacks are practical," in *Proc. 12th Conf. USENIX Secur. Symp.*, vol. 12. Berkeley, CA, USA, 2003, pp. 1–13.

[7] D. Genkin, A. Shamir, and E. Tromer, "RSA key extraction via low-bandwidth acoustic cryptanalysis," in *Advances in Cryptology—CRYPTO*. Berlin, Germany: Springer, 2014, pp. 444–461.

[8] C. Clavier, D. Marion, and A. Wurcker, "Simple power analysis on AES key expansion revisited," in *Cryptographic Hardware and Embedded Systems—CHES*. Berlin, Germany: Springer, 2014, pp. 279–297.

[9] E. Brier, C. Clavier, and F. Olivier, "Correlation power analysis with a leakage model," in *Cryptographic Hardware and Embedded Systems—CHES*, M. Joye and J.-J. Quisquater, Eds. Berlin, Germany: Springer, 2004, pp. 16–29.

[10] S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks: Revealing the Secrets of Smart Cards*. Heidelberg, Germany: Springer, 2007.

[11] M. Bucci, L. Giancane, R. Luzzi, and A. Trifiletti, "Three-phase dual-rail pre-charge logic," in *Cryptographic Hardware and Embedded Systems*. Berlin, Germany: Springer, 2006, pp. 232–241.

[12] D. Sokolov, J. Murphy, A. Bystrov, and A. Yakovlev, "Design and analysis of dual-rail circuits for security applications," *IEEE Trans. Comput.*, vol. 54, no. 4, pp. 449–460, Apr. 2005.

[13] 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. (ESSCIRC)*, Sep. 2002, pp. 403–406.

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

[15] O. Reparaz, B. Bilgin, S. Nikova, B. Gierlichs, and I. Verbauwhede, "Consolidating masking schemes," in *Advances in Cryptology—CRYPTO* (Lecture Notes in Computer Science), vol. 9215. Heidelberg, Germany: Springer, 2015, pp. 764–783. [Online]. Available: http://dx.doi.org/10.1007/978-3-662-47989-6_37

[16] T. Popp, M. Kirschbaum, T. Zefferer, and S. Mangard, "Evaluation of the masked logic style MDPL on a prototype chip," in *Cryptographic Hardware and Embedded Systems—CHES* (Lecture Notes in Computer Science), vol. 4727. Heidelberg, Germany: Springer, 2007, pp. 81–94.

[17] W. Yu and S. Köse, "A lightweight masked AES implementation for securing IoT against CPA attacks," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 64, no. 11, pp. 2934–2944, Nov. 2017.

[18] T. Güneysu and A. Moradi, "Generic side-channel countermeasures for reconfigurable devices," in *Cryptographic Hardware and Embedded Systems—CHES* (Lecture Notes in Computer Science), vol. 6917. Heidelberg, Germany: Springer, 2011, pp. 33–48.

[19] X. Wang *et al.*, "Role of power grid in side channel attack and power-grid-aware secure design," in *Proc. 50th ACM/EDAC/IEEE Design Autom. Conf. (DAC)*, May 2013, pp. 1–9.

[20] A. Shamir, "Protecting smart cards from passive power analysis with detached power supplies," in *Cryptographic Hardware and Embedded Systems—CHES* (Lecture Notes in Computer Science), vol. 1965. New York, NY, USA: Springer-Verlag, 2000, pp. 71–77.

[21] 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.

[22] C. Tokunaga and D. Blaauw, "Secure AES engine with a local switched-capacitor current equalizer," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2009, pp. 64–65.

[23] P. Corsonello, S. Perri, and M. Margala, "An integrated countermeasure against differential power analysis for secure smart-cards," in *Proc. IEEE Int. Symp. Circuits Syst.*, May 2006, pp. 1–4.

[24] M. Kar, D. Lie, M. Wolf, V. De, and S. Mukhopadhyay, "Impact of inductive integrated voltage regulator on the power attack vulnerability of encryption engines: A simulation study," in *Proc. IEEE Custom Integr. Circuits Conf.*, Sep. 2014, pp. 1–4.

[25] A. Singh, M. Kar, J. H. Ko, and S. Mukhopadhyay, "Exploring power attack protection of resource constrained encryption engines using integrated low-drop-out regulators," in *Proc. IEEE/ACM Int. Symp. Low Power Electron. Design (ISLPED)*, Jul. 2015, pp. 134–139.

[26] A. Singh, M. Kar, A. Rajan, V. De, and S. Mukhopadhyay, "Integrated all-digital low-dropout regulator as a countermeasure to power attack in encryption engines," in *Proc. IEEE Int. Symp. Hardw. Oriented Secur. Trust (HOST)*, May 2016, pp. 145–148.

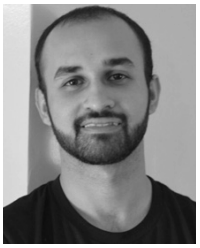
[27] M. Kar, A. Singh, S. Mathew, A. Rajan, V. De, and S. Mukhopadhyay, "Exploiting fully integrated inductive voltage regulators to improve side channel resistance of encryption engines," in *Proc. Int. Symp. Low Power Electron. Design*, New York, NY, USA, 2016, pp. 130–135.

[28] M. Kar, A. Singh, S. Mathew, A. Rajan, V. De, and S. Mukhopadhyay, "Improved power-side-channel-attack resistance of an AES-128 core via a security-aware integrated buck voltage regulator," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2017, pp. 142–143.

[29] M. Kar, A. Singh, A. Rajan, V. De, and S. Mukhopadhyay, "An integrated inductive VR with a 250 MHz all-digital multisampled compensator and on-chip auto-tuning of coefficients in 130 nm CMOS," in *Proc. 42nd Eur. Solid-State Circuits Conf. (ESSCIRC)*, Sep. 2016, pp. 453–456.
[30] O. A. Uzun and S. Köse, "Converter-gating: A power efficient and secure on-chip power delivery system," *IEEE J. Emerg. Sel. Topics Circuits Syst.*, vol. 4, no. 2, pp. 169–179, Jun. 2014.
[31] W. Yu and S. Köse, "Charge-withheld converter-reshuffling: A countermeasure against power analysis attacks," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 63, no. 5, pp. 438–442, May 2016.
[32] W. Yu and S. Köse, "A voltage regulator-assisted lightweight AES implementation against DPA attacks," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 63, no. 8, pp. 1152–1163, Aug. 2016.
[33] W. Yu, O. A. Uzun, and S. Köse, "Leveraging on-chip voltage regulators as a countermeasure against side-channel attacks," in *Proc. 52nd ACM/EDAC/IEEE Design Autom. Conf. (DAC)*, Jun. 2015, pp. 1–6.
[34] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Trans. Comput.*, vol. 51, no. 5, pp. 541–552, May 2002.
[35] 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.
[36] S. B. Nasir, S. Sen, and A. Raychowdhury, "A 130 nm hybrid low dropout regulator based on switched mode control for digital load circuits," in *Proc. 42nd Eur. Solid-State Circuits Conf. (ESSCIRC)*, Sep. 2016, pp. 317–320.

Debayan Das (S'17) received the B.E. degree in electronics and telecommunication engineering from Jadavpur University, India, in 2015. He is currently pursuing the Ph.D. degree with the SPARC Lab, Purdue University, West Lafayette, IN, USA. He was an Analog Design Engineer with xSi Semiconductors (start-up) for a year. His research interests include hardware security and mixed-signal IC design. He was a recipient of the IEEE HOST Best Student Paper Award in 2017.

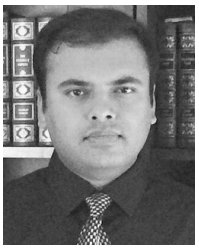
Shovan Maity (S'18) received the B.E. degree in electronics and telecommunication engineering from Jadavpur University, India, in 2012, and the M.Tech. degree in electrical engineering from IIT Bombay, in 2014. He was an Analog Design Engineer at Intel, Bangalore, India, from 2014 to 2016. He is currently pursuing the Ph.D. degree in electrical engineering with Purdue University, West Lafayette, IN, USA. His research interests include design of circuits and systems for human body communication, hardware security, and mixed signal circuits design.



Saad Bin Nasir (M'18) received the B.S. degree in electrical engineering from the National University of Sciences and Technology, Islamabad, Pakistan, in 2010, and the M.S. and Ph.D. degrees in electrical and computer engineering from the Georgia Institute of Technology, Atlanta, GA, USA, in 2014 and 2017, respectively.

His industry experience includes over three years as a Design Engineer at Center for Advanced Research in Engineering, Islamabad, Pakistan, and as a Research Intern at Intel Labs, Intel Corporation, Hillsboro, OR, USA, and also with Qualcomm Inc., San Diego, CA, USA. In 2018, he joined Qualcomm Inc., where he is involved in the design of power management integrated circuits. He has authored/co-authored over 20 journal and conference publications. His research interests include analog/digital/mixed-signal circuit design for power management in high-performance servers, mobile devices, and Internet of Things. He was a recipient of the 2013–2014 Fulbright Fellowship, the 2016–2017 International Solid-State Circuits Society Pre-Doctoral Achievement Award, the Best Student Paper Awards at 2017 HOST, 2016 and 2017 TECHCON conferences. He was a Finalist of 2015 DAC Ph.D. forum and the 2015 Qualcomm Innovation Fellowship.

Santosh Ghosh received the Ph.D. degree from the Department of Computer Science and Engineering, IIT Kharagpur, in 2011. He was a Post-Doctoral Researcher at COSIC, KU Leuven. He is currently at Intel Labs, Intel Corporation, OR, USA. He has over 30 research publications and 20 filled patents in USA. His areas of interest include cryptography, hardware security, security for IoT, and autonomous driving.



Arijit Raychowdhury received the Ph.D. degree in electrical and computer engineering from Purdue University in 2007. His industry experience includes five years as a Staff Scientist with Intel Labs, and a year as an Analog Circuit Researcher with Texas Instruments Inc. He joined the Georgia Institute of Technology, Atlanta, GA, USA, in 2013, where he is currently the ON Semiconductor Jr. Associate Professor with the School of Electrical and Computer Engineering. He is the Associate Director of the Center for Co-Design of Chips, Packaging and Systems. He holds over 25 international patents and has authored over 150 refereed articles. His research interests include low power digital and mixed-signal circuit design. He received the SRC Technical Excellence Award in 2005, the Best Thesis Award, College of Engineering, Purdue University in 2007, the Dimitris N. Chorafas Award for Outstanding Doctoral Research in 2007, the Intel Labs Technical Contribution Award in 2011, the Intel Early Career Award in 2015, the NSF CISE Research Initiation Initiative Award in 2015, the Georgia Tech Outstanding Junior Faculty Award in 2018, and several best paper awards.

Shreyas Sen (S'06–M'11–SM'17) received the Ph.D. degree in electrical and computer engineering from the Georgia Institute of Technology, Atlanta, GA, USA, in 2011. He has over five years of industry experience as a Research Scientist with the Circuit Research Lab and Wireless Communication Research, Intel Labs, and as a Research Intern with Qualcomm and Rambus. He is currently an Assistant Professor with the School of Electrical and Computer Engineering, Purdue University. He has authored/co-authored two book chapters, over 100 journal and conference papers and has 13 patents granted/pending. His research interests include mixed-signal circuits/systems for Internet of Things, biomedical, and security.

Dr. Sen was a recipient of the Young Engineering Fellowship in 2005, the GSRC Margarida Jacome Best Research Award in 2007, the SRC Inventor Recognition Award in 2008, the RWS Best Paper Award in 2008, the IEEE Microwave Fellowship in 2008, the Intel PhD Fellowship in 2010, the Intel Labs Quality Award in 2012, the ICCAD Best-in-Track Award in 2014, the VTS Honorable Mention Award in 2014, the Intel Labs Divisional Recognition Award in 2014 for industry-wide impact on USB-C type, the NSF CISE CRII Award in 2017, the AFOSR Young Investigator Award in 2017, the Google Faculty Research Award in 2017, the HOST Best Student Paper Award in 2017, and the MIT TR35 India Award in 2018. He serves/has served as an Associate Editor for the IEEE DESIGN & TEST, an Executive Committee Member of the IEEE Central Indiana Section, ETS, and a Technical Program Committee Member of DAC, DATE, ICCAD, ITC, VLSI Design, IMSTW, and VDAT.