Reducing Power Side-Channel Information Leakage of AES Engines Using Fully Integrated Inductive Voltage Regulator

Monodeep Kar, *Member, IEEE*, Arvind Singh, *Student Member, IEEE*, Sanu K. Mathew, *Fellow, IEEE*, Anand Rajan, Vivek De, *Fellow, IEEE*, and Saibal Mukhopadhyay, *Fellow, IEEE*

***Abstract*— This paper demonstrates an integrated inductive voltage regulator (IVR) for improving power side-channel-attack (PSCA) resistance of 128-bit Advanced Encryption Standard (AES-128) engines. An inductive IVR is shown to transform the current signatures generated by an encryption engine. Furthermore, an all-digital circuit block, referred to as the loop-randomizer, is introduced to randomize the IVR transformations. A 130-nm test-chip with an inductive IVR with 11.6-nH inductance, 3.2-nF capacitance, and 125-MHz switching frequency is used to drive two different architectures of AES-128 engine: high performance and low power. The measurements demonstrate that the IVR with loop randomizer eliminates information leakage while incurring only 3% overhead in performance and 5% overhead in power over a baseline IVR-AES system. Moreover, while a key-byte can be extracted for the standalone high-performance and low-power AES (LP-AES) with only 5000 and 1000 measurements, respectively, the proposed IVR inhibits key extraction even with 500 000 measurements.**

***Index Terms*— Advanced Encryption Standard (AES), correlation power analysis (CPA), countermeasure, information leakage, integrated voltage regulator, power attack, side-channel-attack, template attack, test vector leakage assessment (TVLA).**

I. Introduction

SPECIALIZED instructions and/or hardware accelerators for Advanced Encryption Standard (AES) cipher are increasingly being used in many high performance processors, such as Intel Haswell/Skylake [1], IBM z9/z10 [2], and ARM A-64, to support bulk encryption. Likewise, many IoT devices include encryption to ensure secure communications. Improving performance and/or reducing power dissipation of encryption engines, while preserving the security/integrity of the key, has emerged as an important challenge for SoC design.

Manuscript received September 3, 2017; revised January 12, 2018 and March 19, 2018; accepted March 19, 2018. Date of publication May 21, 2018; date of current version July 20, 2018. This paper was approved by Associate Editor Marian Verhelst. This work was supported in part by the Intel Corporation, in part by the National Science Foundation under Grant 1218745, and in part by the Semiconductor Research Corporation under Grant 1836.110. *(Corresponding author: Monodeep Kar.)*

M. Kar, S. K. Mathew, A. Rajan, and V. De are with the Intel Labs, Hillsboro, OR 97124 USA (e-mail: monodeep.kar@intel.com; sanu.k.mathew@intel.com; anand.rajan@intel.com; vivek.de@intel.com).

A. Singh and S. Mukhopadhyay are with the Department of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA 30332 USA (e-mail: rathorearvind19@gatech.edu; saibal.mukhopadhyay@ece.gatech.edu).

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/JSSC.2018.2822691

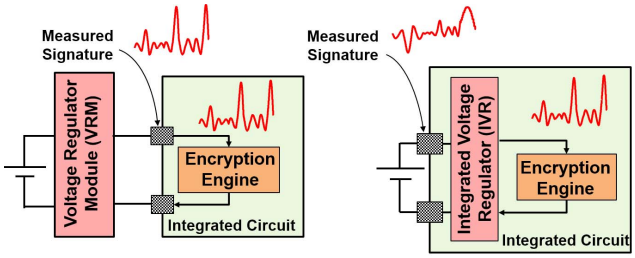

Fig. 1. Effect of an integrated voltage regulator on measurement of power signatures.

The encryption algorithms like AES are secure against traditional cryptanalysis-based key extraction; however, the hardware accelerators are vulnerable to side-channel attack (SCA) [3]. In a SCA, an adversary exploits the information leakage through different measurable physical quantities (side channels) of the hardware engine, such as power dissipation or electromagnetic emission. The power side-channel attack (PSCA), which has emerged as a major threat, exploits the inherent correlation between power dissipation and bit patterns (i.e., switching activity) in digital circuits. An adversary measures the power (supply current) consumed by the target hardware platform and applies statistical analysis techniques to predict the secret key.

To inhibit PSCA, several past research efforts have developed: 1) algorithm/architecture techniques to modify the intermediate computation steps of the algorithms [4], [5] and 2) logic level techniques to ensure that the supply current is independent of the inputs to the logic gates [6], [7]. However, the existing countermeasures incur significant penalties in power and/or performance. Moreover, the countermeasures are often unique to an algorithm or hardware architecture, and do not provide a generic solution. Consequently, there is a growing interest in generic techniques that seek to decorrelate the measured input current signatures from the power signatures of encryption engines with minimal changes to algorithmic/logic/physical implementation. Current equalization [8], noise injection in power distribution network (PDN) [9], and clock randomization [10] are examples of such generic techniques.

This paper presents a generic and low-overhead technique for improving PSCA robustness by exploiting on-chip voltage

regulators present in the state-of-the-art SoCs. Integration of inductive voltage regulators in the same die with a digital logic using on-chip or interposer-based inductors has shown to improve power management in modern SoCs and processors [11]–[13]. From the perspective of PSCA, integrated voltage regulators (IVRs) shield the internal supply node of the AES engines (Fig. 1). The load current signatures generated by a digital logic are now transformed through an IVR before being measured at the IVR's input. Hence, IVR's input current shows poor correlation with the load current, suggesting that an IVR can be exploited to improve PSCA resistance. The recent simulation-based works have explored improvement of PSCA resistance using low-dropout (LDO) regulators [14], [15] and random gating of converters in a multi-phase switched capacitor converter (SCC) [16], [17]. Our prior works have shown that inductive IVRs also can reduce the correlation between the load current signature and the input current signature [18], [19]. However, all of the prior works only performed simulation, and studied whether a baseline IVR can reduce correlation and make key extraction difficult, without quantifying information leakage.

This paper experimentally demonstrates improved PSCA resistance of 128-bit AES engines using a high-frequency inductive IVR. We identify the key transformations through an inductive IVR that can help reduce power side-channel information leakage of AES engines. Moreover, we propose an all-digital synthesizable low-overhead circuit which randomizes the IVR transformations (loop randomizer, LR) and improves the side-channel resistance over the baseline-IVR design.

A 130-nm test chip is designed containing a 125-MHz IVR using 11.6-nH wirebond inductance and 3.2-nF capacitance, powering two 128-bit AES engines, one for high performance and one for low-power operations. We perform test vector leakage assessment (TVLA) [20] tests, correlation power analysis (CPA), and propose a new template-based CPA attack on the randomized IVR mode. TVLA, an emerging standard for PSCA analysis, quantifies the information leakage in a design, while CPA quantifies how many measurement traces are necessary to extract one or more bytes of the secret key. Measurement results demonstrate that the AES engines, when powered without the IVR, show strong TVLA leakage and are vulnerable to a CPA [recovery of at least one successful key-byte after 5000 measurements for the high-performance AES (HP-AES) and 1000 measurements for the low-power AES (LP-AES)]. However, when both the AES designs are powered by the IVR after turning on the proposed loop-randomizer block, the TVLA leakage at the IVR input is reduced below the leakage threshold, and no successful CPA was observed even with 500 000 measurements.

The rest of this paper is organized as follows. Section II discusses the transformations introduced by an IVR. Section III presents the test chip design. Section IV presents the measurement results. Section V discusses potential threat models. Finally, Section VI concludes this paper.

II. Transformations of an Inductive IVR

Fig. 2(a) shows a simplified diagram of an inductive buck regulator. The power stage of the IVR, consisting of switches M_1 and M_2, is switched by square waves with duty cycle set by a pulsewidth modulator (PWM). The switching node (V_{SW}) is filtered by the output filter consisting of an inductance and a capacitance. Compared to off-chip VRs, the IVRs use much smaller passives ($L < 10$ nH, $C < 20$ nF), coupled with high (>100 MHz) switching frequency. A voltage mode controller compares the output voltage V_{OUT} to a reference voltage V_{REF} and compensates the error by changing the duty cycle for the PWM. The IVR introduces following key transformations to the load current signature.

A. Large Signal Transformation

The power stage of the IVR continuously switches and creates a pulsating current pattern at the IVR input current irrespective of whether the IVR load current is changing or not [Fig. 2(b)]. The parasitic inductance (L_{PKG}) and resistance (R_{PKG}) of the chip package and the on-chip decoupling capacitance (C_{DECAP}) further distort the pulsating current due to resonance. One of the most effective contributions of the large signal transformation is hiding the start of an encryption event (important for triggering the measurement) as the change in switching current at the IVR input, which is significantly higher in magnitude than the current of the encryption engine and is effective in hiding the current signature.

B. Small Signal Transformation

Fig. 2(c) shows the simplified small signal representation of the IVR (assuming no perturbations in V_{REF} and V_{IN}). The input current (I_{in}) and its small signal component can be expressed as

$$\begin{aligned} I_{in} &= (I_L + i_l)(D + d) \\ I_{IN} &= I_L D \\ i_{in} &= i_l * D + d * I_L = i_l * D + d * I_O \end{aligned} \tag{1}$$

where i_{in}/I_{IN}, i_l/I_L, and d/D are the small signal/average values (over a switching cycle) of the IVR input current, inductor current, and the duty cycle, respectively. The average value of the inductor current (I_L) can also be approximated as the dc value of the load current supplied by the IVR (I_O). The two distinct components of (1) represent two small signal paths through which the load current signature propagates from load to input. When M_1 is ON, i_{in} can be approximated as i_l. Therefore, turn on-time of M_1 acts as a window through which the load current signatures leak from IVR output node to IVR input node, representing the first term in (1). The duty cycle of the square waves generated by the compensator represents another small signal path for information leakage, represented by the second term in (1). The current signature of the IVR load (encryption engine) generates voltage perturbations at V_{OUT} node due to non-zero impedance looking into the IVR (z_{out}). The voltage signature propagates through the control path and is modified by the compensator transfer function. As the zero created by the output capacitor (C_{OUT} and R_C) reside at a high frequency for an inductive IVR, small signal gain of the feedback path

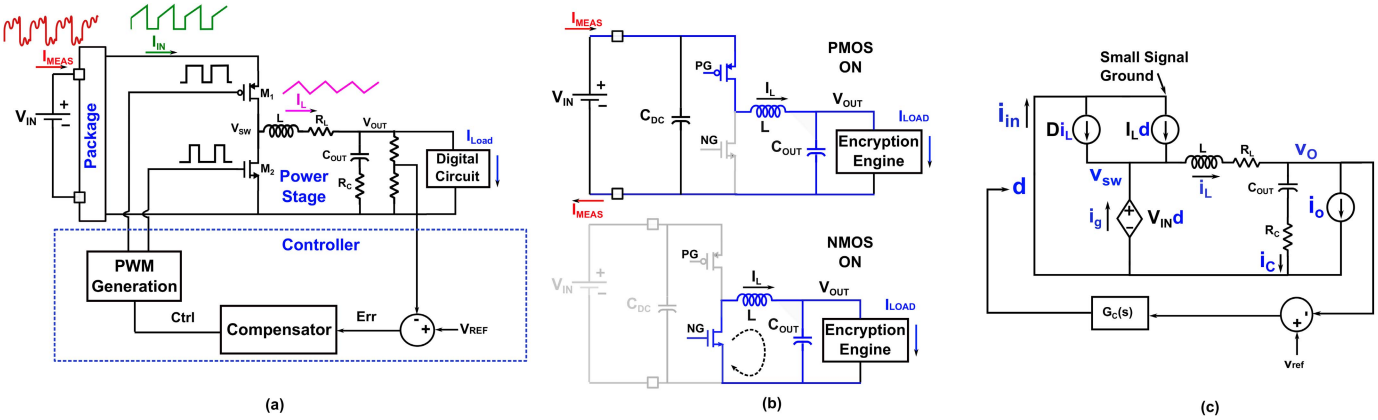

Fig. 2. (a) Circuit diagram of an inductive IVR. (b) Large signal transformation through an IVR. (c) Small signal representation of the control loop of an IVR.

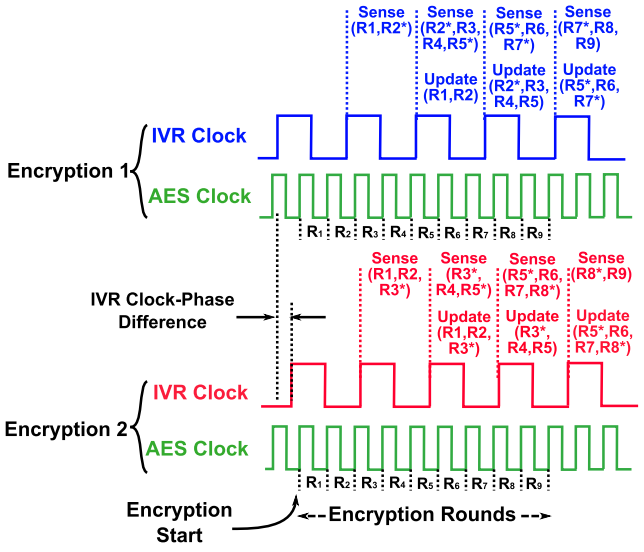

Fig. 3. Misalignment effect in the captured input signatures due to asynchronous nature of the IVR switching clock and the digital clock.

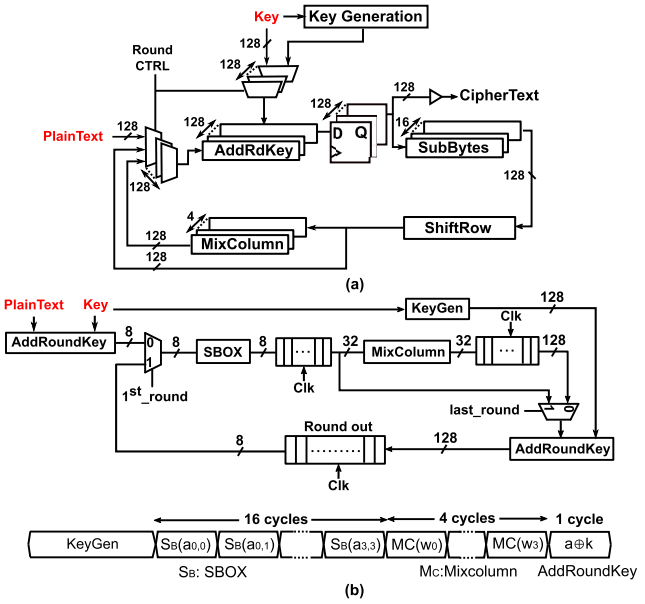

Fig. 4. Architecture of the implemented AES engines. (a) HP-AES. (b) LP-AES.

needs to have two zeroes and two poles to compensate for the phase shift across the power stage. The conversion delay of the ADC (one clock cycle for the implemented design) adds a pole and a type III compensator with two zeroes and one pole is used (as given in the following equation). Evidently, the *small signal transformation* is dictated by the values of the compensator coefficients (b_l and b_2 in the following equation):

$$G_C(z) = \frac{\text{Ctrl}(z)}{\text{Err}(z)} = \frac{b_0 + b_1 z^{-1} + b_2 z^{-2}}{1 - z^{-1}}. \quad (2)$$

C. Misalignment

Successful key extraction attacks like CPA or differential power analysis (DPA) rely on the fact that the measurements are aligned with respect to the rounds of the algorithm. This ensures that the same step of the algorithm is executed at a given sample point across all the measurements. For an IVR powered encryption engine, the encryption clock (ENC_{CLK}) is asynchronous with respect to the IVR switching clock (IVR_{CLK}). Fig. 3 shows the IVR_{CLK} and ENC_{CLK} for two encryption events. Due to the asynchronous nature between these two clocks, each recorded measurements at the IVR input will have different delays between the encryption rounds (R_i in Fig. 3) and the corresponding next IVR clock edge. The leakage through the control path depends on the relative positioning of the IVR clock edges and the encryption rounds, and this relationship is unique for each measurement. The misalignment effect impedes the attacker to extract useful information from the measurements using correlation.

III. System Architecture

A. AES Architecture

Two 128-bit AES architectures have been implemented in the test chip. A 128-bit AES encryption has 10 rounds, each

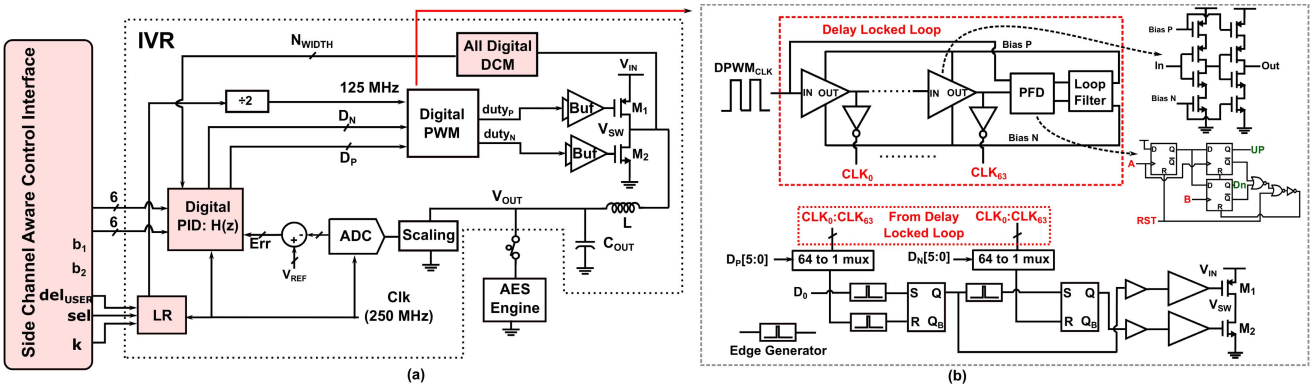

Fig. 5. (a) IVR architecture with an all-digital controller. (b) Details of DPWM engine.

round consisting of four operations (add round key, substitution box, shift rows, and mix column) except for the last round which does not have mix column. The first architecture, adopted from [21], is referred to as HP-AES. Each round is executed in one cycle and all 16 bytes of the intermediate state are processed in parallel [Fig. 4(a)] (11 cycles latency). Due to simultaneous processing of the bytes of the intermediate states, no intermediate storage is required.

The second AES architecture is suited for a low-power application [Fig. 4(b)], referred to as LP-AES. The architecture is similar to [22], however, the traditional GF(2^8) field is used for computation. The datapath consists of a single SBOX, 128 XORs for add round key, a word mix-column unit, and intermediate registers for data storage [Fig. 4(b)]. The round keys for both architectures are generated on the fly (no storage) and the key generation hardware, separate for each design, is synthesized as a part of the main AES core.

B. Baseline IVR

A digitally controlled voltage-mode IVR is designed [Fig. 5(a)]. The design is described in detail in [23].

1) Power Stage: The power stage of the IVR consists of a 11.6-nH inductance and a 3.2-nF capacitance, switched at a 125-MHz frequency, as shown in Fig. 5(a). The inductance is realized using two bondwires of the ceramic leadless chip carrier (CLCC) package, connected in series whereas the capacitance is realized using on-chip metal-insulator-metal (MIM) capacitance.

2) Controller: The IVR uses a digital control loop consisting of a 4-bit ADC and a type III proportional–integral–derivative (PID) compensator. The ADC and the compensator are clocked at 250 MHz, sampling the output twice in one IVR switching period. The multi-sampling approach improves the IVR bandwidth by reducing the delay between sensing and actuation. The ADC has a delay line-based architecture which is suitable for an all-digital synthesizable low-power system [24]. The PID uses a reduced coefficient precision (6-bit) to meet timing.

3) Digital PWM: The digital PWM (DPWM) converts the digital output of the compensator into the duty cycle of the output square wave. The DPWM consists of a delay-locked-loop (DLL) with 64 stages providing a 6-bit resolution.

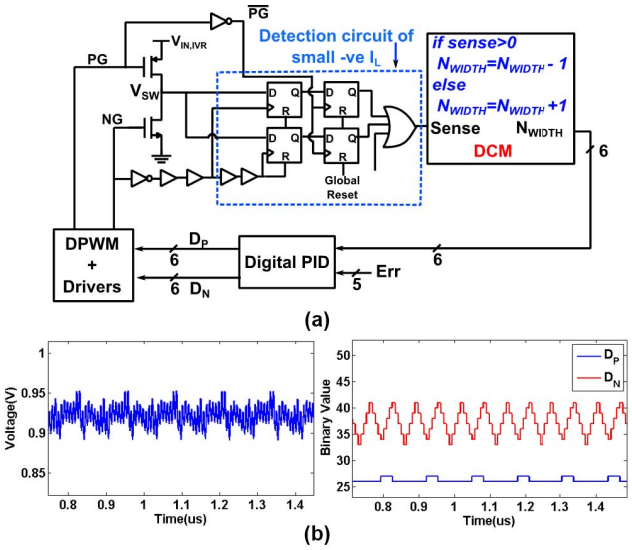

Fig. 6. (a) Circuit and logic for detecting negative inductor current and initiating DCM mode. (b) Waveform of output voltage and the binary value of the PFET and NFET pulse widths (D_P and D_N).

A phase frequency detector [PFD, circuit details in Fig. 5(b)] and a loop filter are used to control the delay of the individual cells.

4) Discontinuous Conduction Mode Engine: An all-digital discontinuous conduction mode (DCM) is used to improve light-load efficiency. The DCM engine senses inductor current and decreases the on-time of M_2 [N_{WIDTH} in Fig. 6(a)], if the sensed current is negative [23]. As soon as the sensed current becomes zero or positive, N_{WIDTH} starts to increment, causing a continuous toggling between the two values of N_{WIDTH} at a steady load current [Fig. 6(b)]. This modifies the large signal transformation as well as the misalignment effect by the IVR.

C. Loop Randomizer in IVR

The PSCA protection offered by the baseline IVR presented in Section III-B solely depends on the transformations described in Section II. The transformations of a baseline IVR, might be partially effective in hiding the information leakage at the IVR input. As the aforementioned transformations are

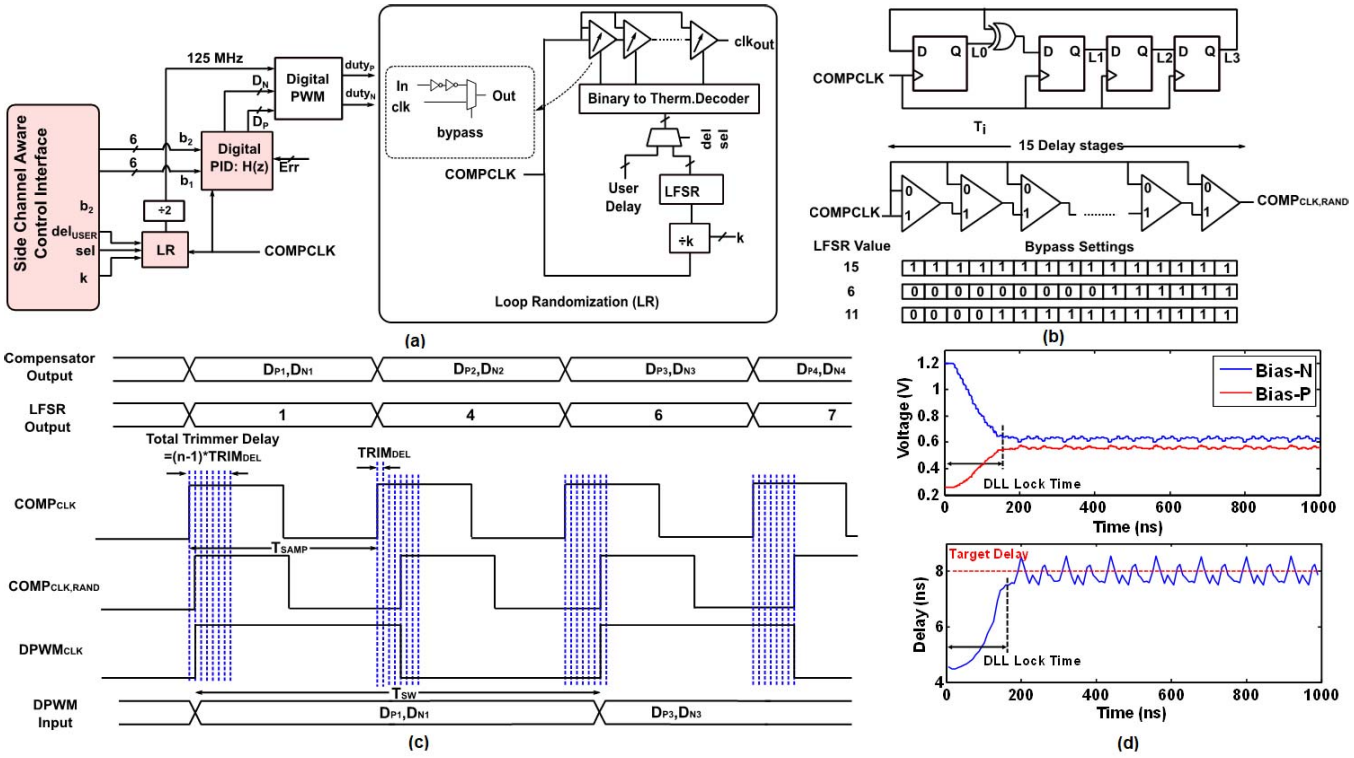

Fig. 7. Design and operation of the loop randomizer. (a) Circuit diagram. (b) Implementation of the 4-bit LFSR and output of the decoder for example LFSR values. (c) Example clock waveforms. (d) Simulated waveforms of DLL internal nodes and the delay across the DLL input and the DLL output clock.

linear time-invariant (LTI) transformations, the input current signature contains a linearly transformed version of the load current signature. Introducing random and dynamic time variance in the IVR transformations can help in reducing PSCA leakage.

1) Design of LR: We propose to introduce time variance in the IVR transformation by delaying the IVR_{CLK} in a pseudo-random fashion. For the proposed architecture, the clock to DPWM is generated from the sampling clock (2× higher frequency) through a clock divider. The input to the clock divider is delayed in a random fashion [Fig. 7(a)]. To achieve this, we have used a delay-trimmer consisting of a series of delay elements, as shown in Fig. 7(b). Each delay element consists of two inverters and one multiplexer. The multiplexer can be used to bypass the delay of the inverters and forward the clock directly to the next stage. The prototype test chip uses 15 such series delay elements. The select of the multiplexers is driven by a binary-to-thermometer decoder. The decoder is driven by a 4-bit maximal length linear feedback shift register [LFSR, Fig. 7(b)]. The LFSR output sequence goes through 15 different values generating 15 different delay values. The thermometer output starts from right as the delay elements in bypass mode bypasses the input clock directly. Fig. 7(c) shows the output clock ($\text{COMP}_{\text{CLK,RAND}}$) waveform assuming a 3-bit LFSR for simplicity. The delay of each trimmer cell is shown as well. $\text{COMP}_{\text{CLK,RAND}}$ is used to generate the $\text{DPWM}_{\text{CLK,RAND}}$ through a clock divider. We note that the compensator outputs D_P and D_N are synchronous with respect to COMP_{CLK} and are captured again with respect to $\text{COMP}_{\text{CLK,RAND}}$ inside the DPWM engine. The extra delay added by the trimmer cells, even when all the cells are in the bypass mode ensures that clock path delay is more than data path delay.

2) Stability Analysis: Randomly delaying the IVR switching clock creates steady-state perturbations at the output voltage of the IVR. It is important to analyze the loop stability of the IVR when LR is turned on. Fig. 7(d) shows the voltage waveforms of the DLL bias nodes [shown in Fig. 5(b)] and the delay between the input and the output clock edges. In the absence of LR, the delay between the DLL's input and output clocks converges to the target delay of 8 ns (corresponding to 125-MHz IVR_{CLK}). However, when LR is turned on, the bias voltages of the DLL as well as the total delay across the delay chain show a bounded oscillation around their corresponding stable values. The upper and the lower limits of the delay can be expressed as

$$T_{\text{DLL,min}} = 2 * T_{\text{SAMP}} - (n-1) * \text{TRIM}_{\text{DEL}}$$
$$T_{\text{DLL,max}} = 2 * T_{\text{SAMP}} + (n-1) * \text{TRIM}_{\text{DEL}} \quad (3)$$

where TRIM_{DEL} is the delay across a single trimmer cell.

For the prototype design, the LR frequency can be adjustable. If LR frequency is kept high, the DLL cannot respond to the delay variations due to limited bandwidth. For a lower LR frequency, the DLL responds to the delay variation. Moreover, as V_{OUT} perturbations are within the control loop bandwidth, the control loop also starts responding to the changes. This results in lower perturbations at the output node.

IV. Measurement Results

The test chip with the IVR and the AES engines was fabricated in 130-nm CMOS. Fig. 8 shows the die photo and the bond wires used for realizing inductance in the IVR power stage. The IVR can convert 1.2-V input to 0.45-V–1-V output. The IVR switching frequency is fixed at 125 MHz as the maximum achievable inductance and capacitance are 11.6 nH and 3.2 nF. The control logic and other configurations are written in the IVR and the AES through two separate serial-to-parallel (SPI) interfaces.

A. Measurement Modes and Environment

Separate pads are created for V_{DD} and V_{SS} of the AES engines to keep the provision of testing the AES engines separately. For the AES, we chose 40 MHz and 0.8 V as the operating condition. A lower clock frequency of the AES engines than the IVR creates a pessimistic scenario for PSCA resistance by reducing the attenuation of the side-channel signatures through the IVR. Side-channel signatures are measured for the following conditions.

1) *Standalone AES:* The AES is powered through the dedicated V_{DD} and V_{SS} pins of the AES engines. Switch S_1 in Fig. 8(c) is kept open. In this mode, the signatures at the V_{AES} node are measured.
2) *Baseline IVR-AES:* Switch S_1 is closed and the IVR output is set to 0.85 V (LR OFF). The IVR drives a high load current created through a synthetic load generator, and therefore, remains in continuous conduction mode (CCM). In this mode, the signatures at the $V_{IN,IVR}$ node are measured.
3) *IVR-AES in DCM:* The IVR output is set to 0.85 V (LR OFF), however, the synthetic load generator is turned off. The IVR moves to the DCM. $V_{IN,IVR}$ signatures are measured.
4) *IVR-AES With LR:* LR is turned on with the IVR in the CCM mode. $V_{IN,IVR}$ signatures are measured.

A series of 1-Ω resistor is inserted in the series path of the AES supply (for standalone AES measurements) and the IVR supply (for IVR-AES measurements) [Fig. 8(c)].

B. Statistical Tests

We have used two different types of statistical tests to quantify PSCA resistance.

1) Test Vector Leakage Assessment: TVLA as proposed by Goodwill *et al.* [20], is a testing methodology which aims to find out whether the side-channel signatures are correlated with the internal power consumption. In TVLA, a tester encrypts two plaintext lists PT_1 and PT_2, with a known key K_T. PT_1 consists of n statistically random inputs. PT_2 consists of n unique inputs, each of which when encrypted with key K_T leads to one of the AES intermediate rounds showing lower power consumption. The measured data set is split into two partitions (X_1 and X_2) and Welch's t-test is performed

$$t = \frac{\mu_{X1} - \mu_{X2}}{\sqrt{\frac{\sigma_{X1}^2}{n} + \frac{\sigma_{X2}^2}{n}}} \tag{4}$$

where μ and σ denote the mean and standard deviation of a data set. A t-value of more than 4.5 for more than 5000 plaintexts in each data set indicates that the power consumption of the target device is correlated with the underlying switching activities.

2) Correlation Power Analysis: The CPA is a well-known side-channel attack to extract the secret key. CPA has been shown to be faster and more accurate than DPA, another popular power attack technique [25]. The minimum number of traces required to extract the key, referred to as the minimum traces to disclosure (MTD) is a metric of PSCA resistance. The power models used in CPA for both AES architectures are explained as follows. Flip-flops are targeted for the attack instead of combinational logic, as the data-dependency in the power consumption (transition of the output bits) is aligned with respect to the clock edge.

a) Power model selection: i) HP-AES: The Hamming distance between the intermediate state at the end of the penultimate round (9th) and the last round of the encryption is used to create a power model (16 power models for 16 bytes of the key). The power model correlates with the dynamic power consumption of the eight flip-flops of the 128-bit register that stores the intermediate state/ciphertext.

ii) LP-AES: The Hamming weight of the SBOX output in the first round is chosen as power model. The SBOX operation on each byte is executed serially in LP-AES and the SBOX outputs are stored back to the intermediate storage; therefore, the power model is expected to correlate with the flip-flop power.

3) Frequency Domain CPA: We also perform frequency domain CPA which can break time-shift/desynchronization-based countermeasures. The phase shift of the signatures through the IVR transformations does not affect the magnitude information in any frequency domain representation [fast Fourier transform (FFT), spectrogram, and discrete wavelet transform (DWT)] and the same power model can be used for CPA. A window-based FFT is performed where the window length is optimized to capture localized changes while ensuring it is large enough such that the signatures of interest remain within the chosen window even after the worst case time shift.

C. Sample Waveforms

Fig. 9(a) shows the signature on V_{AES}, when the HP-AES is powered externally along with the corresponding AES clock. The 10-round operation of the AES is distinctly visible. Fig. 9(b) shows the signature on $V_{IN,IVR}$ during an AES encryption, when the AES is supplied by the baseline IVR. The AES rounds are not visible in the $V_{IN,IVR}$ signature. Therefore, identifying the AES operation from the $V_{IN,IVR}$ signature is difficult.

Fig. 10(a) shows the signature on V_{AES} when the LP-AES is powered externally. Compared to the HP-AES, the rounds are not clearly visible as the computation is distributed over 500 cycles, which reduces the power consumed per clock cycle. However, filtering the V_{AES} signatures using a bandpass filter (70–90 MHz covering the clock

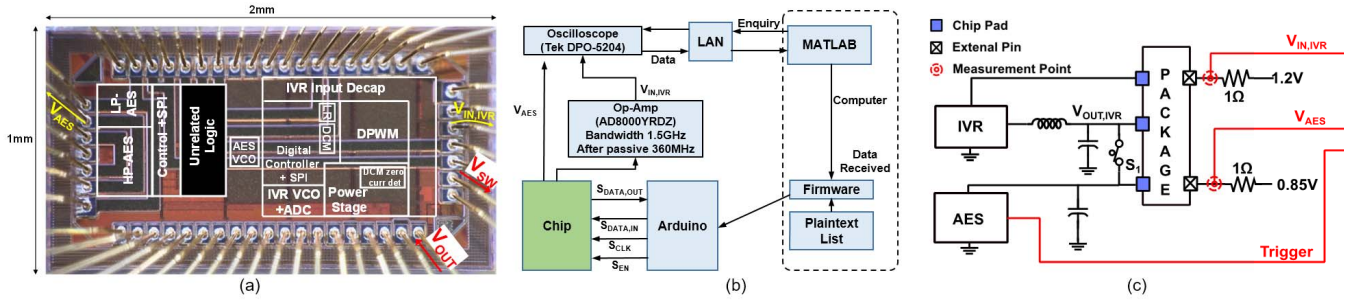

Fig. 8. (a) Micrograph of the fabricated test-chip. (b) Setup for side-channel measurement. (c) Measurement points.

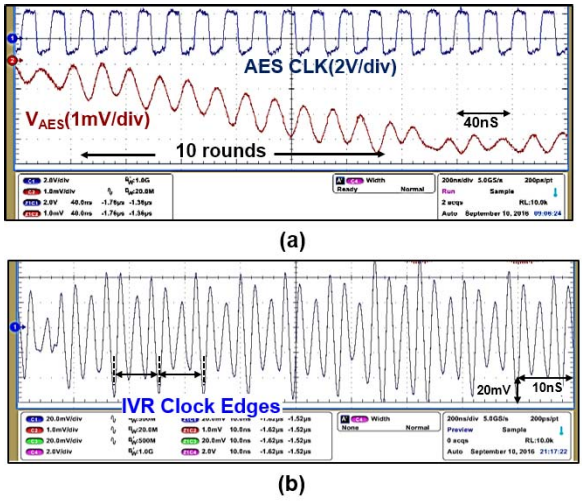

Fig. 9. PSCA signatures of the HP-AES. (a) V_{AES} in standalone mode. (b) $V_{IN,IVR}$ for baseline IVR-AES.

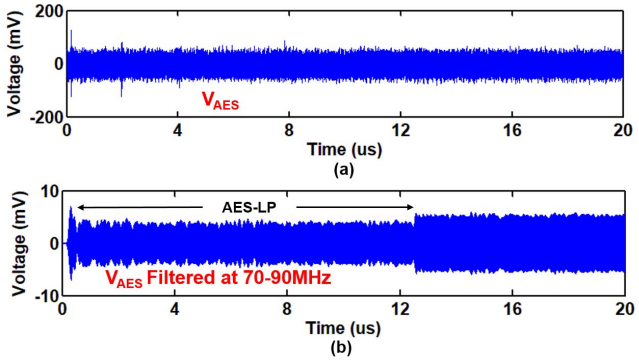

Fig. 10. PSCA signatures of the LP-AES. (a) V_{AES} in standalone mode. (b) Filtered V_{AES} shows the AES operation.

double harmonic at 80 MHz) distinguishes the AES operation [Fig. 10(b)]. The $V_{IN,IVR}$ signatures are similar to the HP-AES and are not shown for brevity.

1) Effect of LR: When LR is turned on, the IVR edges are randomly delayed as shown in Fig. 11. The LR block can be driven at different frequencies, ranging from F_{SAMP} to $F_{SAMP}/8$, F_{SAMP} being the sampling frequency of the controller (ADC and compensator). Slowing the LR frequency

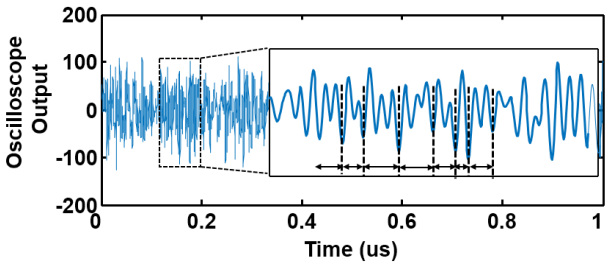

Fig. 11. $V_{IN,IVR}$ signature with active LR.

reduces both the output ripple as well as frequency spreading in the input current. Fig. 12(a) shows the normalized output ripple without the LR and with LR at different frequencies. As the LR frequency is lowered, the output ripple decreases. Fig. 12(b) and (c) show the $V_{IN,IVR}$ spectrum for the maximum and the minimum LR frequencies used in the design. When LR is running at F_{SAMP}, the maximum spreading is observed at the $V_{IN,IVR}$ spectrum as the output perturbation is outside the loop bandwidth. More frequency spreading helps in obfuscating the PSCA signatures, however, the output ripple also increases. For the demonstrated results, the LR is driven at $F_{SAMP}/8$.

D. Post-Processing and Alignment

The trigger used in the measurement setup [Fig. 8(c)] is not synchronous with respect to both the IVR_{CLK} and the ENC_{CLK}; therefore, alignment is required for both standalone as well as IVR-AES configurations for TVLA and CPA. For standalone AES, the V_{AES} signatures are filtered using a bandpass filter with center frequency at the ENC_{CLK} and aligned using cross correlation. The alignment process of $V_{IN,IVR}$ signatures is shown in Fig. 13. Here, we assume that the adversary does not have access to V_{AES} and a similar methodology for aligning V_{AES} in a standalone mode is adopted. A series of bandpass filters, with center frequencies varying from 30 to 500 MHz in steps of 10 MHz are used to filter the $V_{IN,IVR}$ signatures and the filtered signatures are aligned using cross correlation, with the correlation offset bounded by the filtering frequency. An alternate alignment process of $V_{IN,IVR}$, which uses the offset from alignment of V_{AES} signatures, is described in [26] and assumes that the V_{AES} node is observable by the adversary. However, using

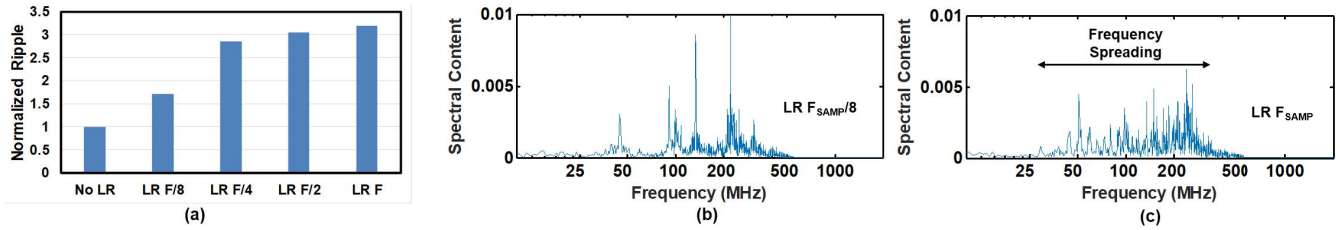

Fig. 12. Effect of LR frequency on (a) ripple magnitude at V_{OUT}/V_{AES} and (b), (c) spectrum of $V_{IN,IVR}$ for two different LR frequencies.

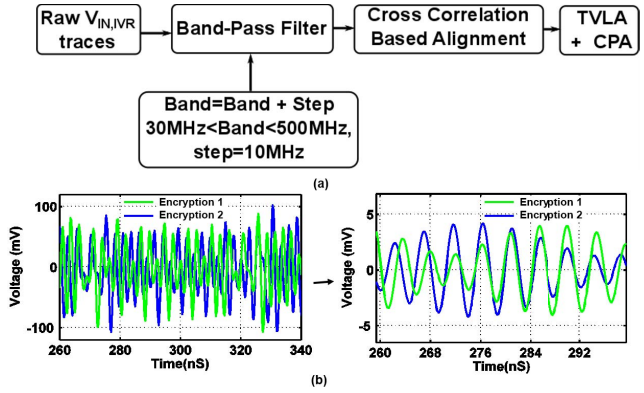

Fig. 13. (a) Alignment process of $V_{IN,IVR}$. (b) $V_{IN,IVR}$ signature before and after alignment.

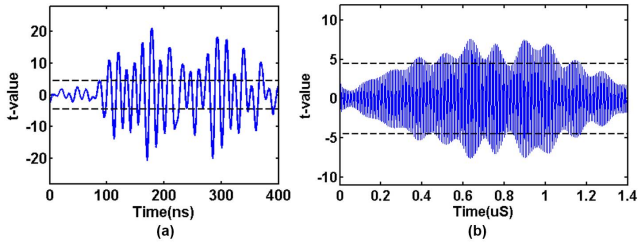

Fig. 14. TVLA on (a) V_{AES} in standalone configuration (b) $V_{IN,IVR}$ for baseline IVR-AES with 125-MHz filtering.

a wider frequency range for filtering with the new alignment method yields similar results as [26] and more importantly, is independent of any assumption about the observability of V_{AES}.

E. High Performance AES

1) Test Vector Leakage Assessment:

a) Standalone: Fig. 14(a) shows the measured t-value against time for the TVLA test of the standalone AES. The t-value crossed the 4.5 threshold at multiple time instants clearly indicating leakage.

For all IVR-AES configurations, TVLA is performed with 50 000 plaintexts in each set.

b) Baseline IVR: For the baseline IVR in the CCM mode, no successful TVLA was observed before alignment (Section IV-D). After the post-processing, different frequency bands, which were used for filtering the $V_{IN,IVR}$ signatures, show different leakage behaviors. Fig. 14(b) shows TVLA results on post-processed $V_{IN,IVR}$ signatures at a 125-MHz frequency band. We note the following observations.

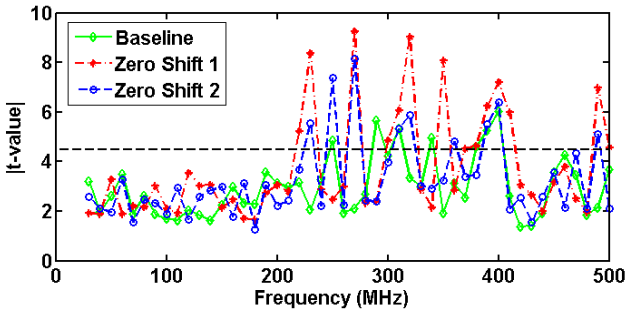

Fig. 15. Peak t-value from TVLA on $V_{IN,IVR}$ for baseline IVR-AES and two different compensator zero locations across the frequency bands used for filtering.

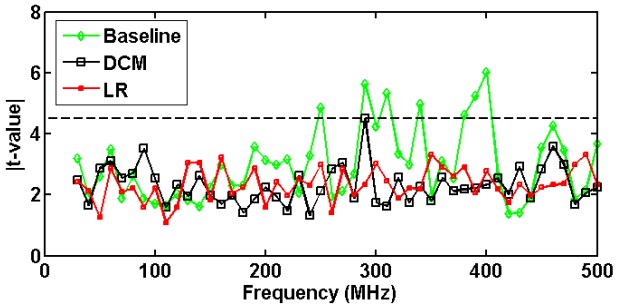

Fig. 16. TVLA results for $V_{IN,IVR}$ in DCM mode and active LR.

1) The t-value at $V_{IN,IVR}$ crosses the 4.5 threshold between 0.4 and 1 μs indicating leakage.
2) The t-value crosses the 4.5 threshold across multiple peaks in the post-processed signal. This is caused by the AES data-dependent signatures getting spread across multiple IVR clock phases (IVR_{CLK}) at the IVR input current.

c) Effect of compensator zero locations: TVLA is repeated for two different zero locations than the baseline IVR. We ensure that the modified zero locations maintained stability of the IVR but the transient (load/reference) response changed. Fig. 15 shows the peak t-value against frequency (center frequency of the filter band used for post-processing) for different zero locations. We note the following observations.

1) For all zero locations, the frequency bands from 200 to 400 MHz show TVLA leakage. This region contains multiple components originating from harmonics of ENC_{CLK} (40 MHz) and IVR_{CLK} (125 MHz) as well as harmonics from different package resonances.
2) The peak t-value across these leaking bands changes as the compensator zero locations change. This is expected

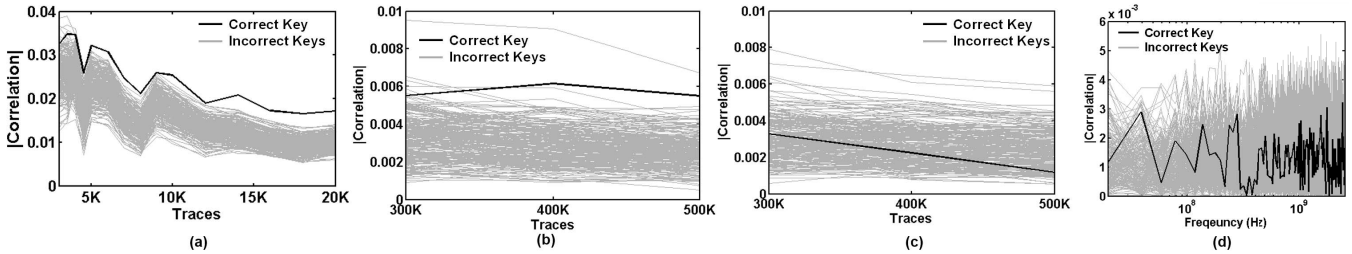

Fig. 17. CPA results on 10th key byte for HP-AES. (a) Correlation against measurements for V_{AES} in standalone mode. (b) Correlation against measurements for $V_{\mathrm{IN,IVR}}$ for baseline IVR-AES mode. (c) Correlation against measurements for $V_{\mathrm{IN,IVR}}$ for active LR. (d) Correlation against frequency for frequency domain CPA for baseline IVR-AES mode.

as changing zero locations change the small signal transformation which controls the leaking frequency bands.

d) DCM: One of the prevalent techniques used by adversaries in improving the signal-to-noise ratio (SNR) of all forms of side-channel measurements is to shut OFF other modules in the processor other than the encryption engine. If an IVR is used to supply multiple digital blocks along with the AES engines, the reduction in load current supplied by the IVR will force the IVR into a DCM mode. More specifically, if the total load current drawn from the IVR reduces below half of inductor current ripple (55 mA at 0.85 V), the IVR would move into a DCM mode. Both the designed AES engines at a 0.85-V supply 40-MHz clock draw <10-mA current, ensuring the previous condition if the AES is the only load to the IVR. Fig. 16 shows that the peak t-value remains below the 4.5 threshold, when DCM is enabled. This is due to the change in the large signal transformation and misalignment in the DCM operation as explained in Section III-B. Therefore, a DCM operation can reduce information leakage irrespective of a higher SNR of measurement.

e) LR: When LR is turned on, all three transformations through the IVR are randomized. Therefore, aligning the $V_{\mathrm{IN,IVR}}$ signatures becomes inaccurate as no constant phase relationship exists between the captured measurements as visible in Fig. 11. Fig. 16 shows that the t-value does not exceed the threshold for all frequency bands.

2) Correlation Power Attack: A leakage test like TVLA indicates presence of data-dependency in the measured side-channel signatures. A successful TVLA does not guarantee a successful key extraction attack like CPA. Therefore, we have also performed CPA on the standalone AES as well as on selected configurations of the IVR-AES system.

a) Standalone AES: The standalone AES, implemented in an unprotected static CMOS, is vulnerable to CPA. The V_{AES} signatures have been filtered and aligned as discussed in Section IV-D. Fig. 17(a) shows the maximum correlation against number of measurements used for computation, for all possible 256 guesses of the 10th key byte. The correlation values of the correct key byte are marked in black and can easily be distinguished after 5000 measurements (MTD of the standalone design).

b) IVR-AES: We first start with performing CPA on the baseline-IVR design. Although TVLA shows leakage across multiple filter bands, no successful CPA was observed across all these bands with the same alignment technique. For TVLA, slices of length 200 ns from the $V_{\mathrm{IN,IVR}}$ signatures were used and post-processed. For CPA, we used slices of 20 ns sliding it across 200 ns in steps of 10 ns, post-processed each of these slices, and performed a CPA. Fig. 17(b) shows correlation against the number of measurements (across all slices and all frequency bands) for the baseline IVR-AES. It is not possible to find out the correct key even with 500 000 measurements; however, the correlation of the correct key is the second highest among all the key guesses, for 500 000 traces. Therefore, it is fair to assume that the MTD of the baseline-IVR design is slightly higher than 500 000. This is an interesting observation as $V_{\mathrm{IN,IVR}}$ in the baseline configuration increases the CPA resistance by $\geq 100\times$, and this improvement in CPA is obtained without any power, performance, and area overhead (as LR is not activated).

Next LR is activated and a CPA is performed on $V_{\mathrm{IN,IVR}}$ [Fig. 17(c)]. Not only no successful CPA was observed with 500 000 measurements, but also the correct key's correlation value does not rank high among the other key guesses. This is coherent with the TVLA results which showed no leakage across all the frequency bands.

c) Frequency Domain CPA: For V_{AES} signatures, a 40-ns window is chosen (across the 9th and 10th peaks in the V_{AES} waveform in Fig. 9) and a successful CPA was observed. For $V_{\mathrm{IN,IVR}}$ signatures, the same window length is chosen to perform the frequency domain conversion as the maximum shift in time is limited by $((1/\mathrm{ENC_{CLK}}) + (1/\mathrm{IVR_{CLK}}) \leq 40$ ns). Fig. 17(d) shows the frequency domain CPA results on the baseline IVR-AES system. No successful CPA was observed on both the baseline IVR-AES and IVR-AES with LR.

F. Low-Power AES

1) Test Vector Leakage Assesment: TVLA on the LP-AES is performed with the same TVLA data set as the HP-AES. As the bytes are processed serially in the LP-AES, the statistical bias in the power consumption is created across four clock cycles (corresponding to the clock cycles which process the bytes satisfying the conditions in [20]).

a) Standalone AES: Fig. 18(a) shows TVLA on V_{AES} in the standalone mode. As the AES is implemented without any countermeasures, TVLA clearly shows signs of leakage.

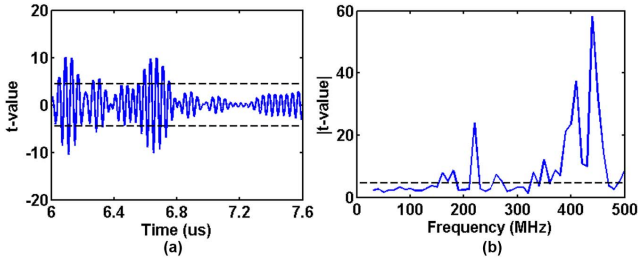

Fig. 18. (a) TVLA on V_{AES} for LP-AES in standalone mode. (b) t-value against filter frequency for $V_{IN,IVR}$ in baseline IVR-AES (50 000 measurements).

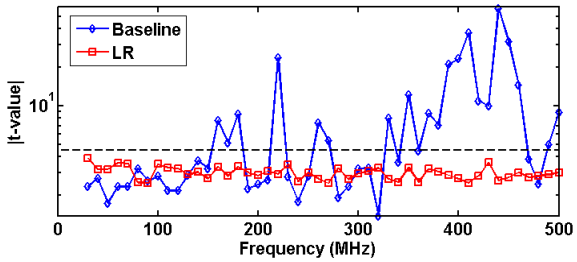

Fig. 19. TVLA on $V_{IN,IVR}$ with active LR against filter frequency (50 000 measurements).

b) Baseline IVR-AES: Fig. 18(b) shows TVLA results for baseline IVR with LP-AES. Consistent with the result for HP-AES, the TVLA shows leakage. Fig. 18(b) shows that the frequency components between 350-500-MHz band show strong leakage. The leaking frequency bands are similar with HP-AES results shown in Fig. 15.

c) IVR-AES with an active LR: Fig. 19 shows TVLA results for IVR-AES with LR activated. No TVLA leakage was observed across all the frequency bands. This shows that LR can be effective in suppressing side-channel leakage for both AES architectures.

2) Correlation Power Analysis: The CPA on LP-AES is carried out with the same plaintext list as HP-AES.

a) Standalone AES: Fig. 20(a) shows the result of CPA on V_{AES} in a standalone mode. Thousand measurements are enough to extract the first key byte using a CPA. When compared to the HP-AES, LP-AES turns out to be $\sim 5\times$ less resistant to a CPA attack. This can be explained due to the serial nature of the computation. For a HP-AES, the power model is expected to correlate with power consumption of eight flip-flops, storing the corresponding byte. However, as the intermediate state is 128-bit wide, the power consumption of the remaining 120 flip-flops acts as noise. In LP-AES, the state of only eight flip-flops is changing during byte serial computation of the SBOX. Therefore, the power consumption correlates perfectly with the power model. This shows that LP-AES or any AES with a serialized datapath is more vulnerable to key extraction attacks.

b) Baseline IVR-AES: $V_{IN,IVR}$ did not show a successful CPA in the baseline-IVR configuration with HP-AES. However, for the LP-AES, the baseline IVR shows a strong CPA, as shown in Fig. 20(b). Thousand and five hundred measurements are enough to extract one of the key-bytes, merely improving the CPA resistance by $1.5\times$ compared to the standalone AES. This is a significant result as it shows that a successful CPA can be performed on $V_{IN,IVR}$ with the same power model used for the standalone AES. As the ENC_{CLK} frequency for the test condition is almost $3\times$ slower than the IVR_{CLK}, information corresponding to one SBOX operation in LP-AES is spread across three IVR cycles. This fact, along with a stronger correlation between the power model and power consumption in LP-AES, explain lower improvement in CPA resistance at $V_{IN,IVR}$.

c) IVR-AES with LR active: Fig. 20(c) shows the CPA result on LP-AES, when LR is activated. No successful CPA was observed with 500 000 measurements. We note that LR successfully increases the CPA resistance of the LP-AES by $\geq 500\times$ from the standalone design and $\geq 330\times$ from the baseline design.

G. Overheads and Comparison

1) F_{MAX} of Encryption Engine: Turning on LR causes the steady-state output ripple to increase and might cause the underlying logic to incur a timing violation. The increased output ripple, shown in Fig. 21(a), reduces the maximum achievable frequency (F_{MAX}) that the encryption engine can run at. Fig. 21(a) also shows the response of V_{OUT} to a sharp load transient before and after activating LR. LR increases the voltage droop by 6 mV and settling time by 30 ns.

To characterize the reduction in F_{MAX}, a large number of AES encryptions are performed before and after turning on LR and the maximum frequency at which all encryptions were executed without functionality failure is found out. Turning on LR causes 3% degradation in F_{MAX} of the AES engines.

2) System Power Overhead: The minimum value in the LFSR sequence can possibly lead to overlapping between the pulse driving M_2 and the pulse driving M_1 for the next cycle [Fig. 21(b)]. To ensure no direct path between V_{IN} and V_{SS}, D_N (Fig. 5) is saturated above a threshold, which ensures that M_2 turns off before the next pulse for M_1 appears. However, when next M_1 pulse appears after $T_{DLL,MAX}$, the inductor current flows through the body diode of M_2 for the longest amount of time, leading to a higher conduction loss. However, the power overhead is significantly lower than the situation when the M_1 and M_2 pulses overlap. For a 60-mA dc current at the IVR output, LR increases the IVR input power by 5%.

3) Performance Comparison: Table I compares the proposed security aware IVR design and its overheads with selected application specified integrated circuit (ASIC)-based generic/logic style-based countermeasures. The low overheads of the security aware IVR design and the ease of integration into an existing IVR design make the proposed techniques attractive for implementation.

4) Existing Power Supply Countermeasures: Securing power supplies for applications with sensitive data have been explored previously both in published papers as well as patents. Shamir proposed to use an internal decoupling capacitor as the power supply during the secure operations of the underlying circuit [29]. However, this method does not

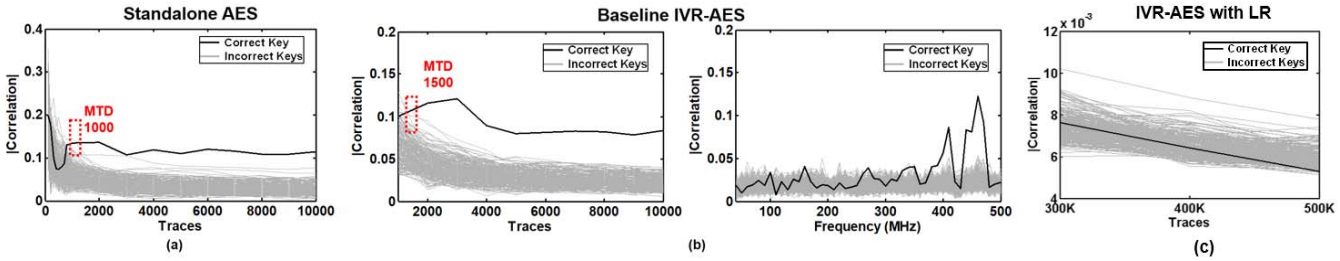

Fig. 20. CPA results on different IVR configurations for LP-AES. (a) Correlation against measurements for V_{AES} in standalone mode. (b) Correlation against measurements and frequency bands for filtering for $V_{\mathrm{IN,IVR}}$ in baseline IVR-AES. (c) Correlation against measurements for $V_{\mathrm{IN,IVR}}$ with LR active.

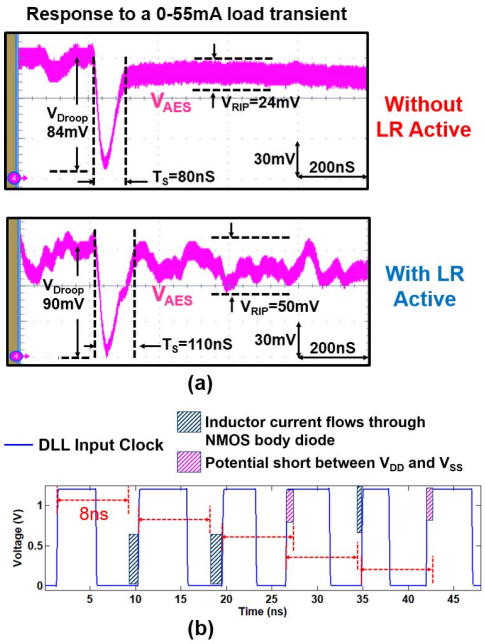

Fig. 21. (a) Steady-state ripple and transient performance without and with LR active. (b) Possible sources of power loss in LR mode.

TABLE I

PERFORMANCE COMPARISON AGAINST SELECTED EXISTING COUNTERMEASURES

Parameter	This Work	VLSI'15 [27]	ISSCC'09 [8]	ISSCC'11 [28]
Technology	130nm	65nm	130nm	130nm
Standalone AES Power/Freq.	10.5mW/ 40MHz	138.1mW/ 1.32GHz	33.32mW/ 100MHz	-/50MHz
Operating Voltage(V)	0.4-1 (from IVR)	1 (External)	1.2 (External)	1.2 (External)
Power Overhead	5%*	-30%	33%	-
Area Overhead	2135um^2 (103 gates)$	6000um^2 (25%)	7900um^2 (20%)	11K gates (67%)
Performance Overhead	3.33%&	0%	50%	0%
Analysis Method	CPA, TVLA	DPA	DPA	CPA/ Fault-Attack

*Total increase in IVR+AES system power after turning on the LR with 60mA parallel load along with AES

$ Area of the synthesized LR block

& Performance overhead calculated from Fmax impact due to higher droop (increase in supply guardband) with LR on

ensure a tight regulation on the supply line of the circuits and requires a relaxed supply guard band to avoid timing failure. In another variation of this technique, Mohel *et al.* [30] uses two intermediate power storage units, one of them supplying to the underlying circuitry and the other one getting charged from the main power supply. Multiple works have proposed various techniques where regulation is maintained at the supply line; however, the current signatures drawn by the circuits are equalized by adding a parallel current branch. Ratanpal *et al.* [31] and Das *et al.* [32] used different variants of this technique to improve the robustness against power attacks. Kim [33] used variable supply decoupling capacitance to equalize the supply current drawn by the digital circuits. For an efficient implementation of this scheme, high-speed comparators are required which would quickly switch between variable capacitances to regulate the supply line. Hernandez *et al.* [34] used a two-stage regulator topology, an isolation charge pump followed by a linear regulator. The data-dependency is reduced through discharging the charge pump capacitance to zero before charging it up. This would significantly reduce the power efficiency of the charge pump. Compared to the existing techniques, the transformations through an inductive IVR are fundamentally different. Moreover, an inductive IVR maintains a tight regulation at the output and the proposed changes are easy to integrate using digital synthesis flow into the IVR architecture without significant power/performance overhead.

V. THREAT MODEL

A. Reversibility Attack

A potential threat model to IVR-based protection is to reverse-engineer the transformations applied by the IVR using an inverse transformation, to recover the AES current pattern from the measured IVR input current pattern and mount the power attack on the predicted current. The large signal transformation, i.e., the switching of the IVR's power stage determines how often the duty cycle command would change for a voltage mode control of an IVR. The turn on time of the transistor M_1 provides a window for V_{AES} signatures to appear at $V_{\mathrm{IN,IVR}}$. The effect of V_{AES} signatures not appearing at $V_{\mathrm{IN,IVR}}$ when M_1 is OFF, cannot be reversed. The small signal transformation introduced in the input current can be modeled, and hence, the attacker can use an inverse transformation to estimate the load current, as discussed next .

1) Current Transformation Through an IVR: The small signal representation of the input current of the IVR has been shown in (2). For the following analysis, V_O/v_o, $V_{\mathrm{SW}}/v_{\mathrm{sw}}$, and $V_{\mathrm{IN}}/v_{\mathrm{in}}$ represent the averaged value/small signal value of the output voltage, the switching node voltage, and the input

voltage, respectively. Equation 2 can be rewritten as

$$i_{\text{in}} = \left(D\frac{i_l}{v_o} + I_0\frac{d}{v_o}\right)v_o. \tag{5}$$

Small signal duty cycle (d), assuming no small signal variation in the reference voltage (v_{ref}), can be written as

$$d = -G_c v_o. \tag{6}$$

Inductor current and its corresponding small signal component can be approximated as

$$I_L = \frac{V_{\text{SW}} - V_O}{sL + R_L} = \frac{DV_{\text{IN}} - V_O}{sL + R_L}$$
$$i_l = \frac{dV_{\text{IN}} + Dv_{\text{in}} - v_o}{sL + R_L}. \tag{7}$$

Assuming no small signal variation in the input voltage (v_{in})

$$i_l = \frac{dV_{\text{IN}} - v_o}{sL + R_L}. \tag{8}$$

Substituting the value of d, the equation can be written as

$$\frac{i_l}{v_o} = -\frac{1}{sL + R_L} \times (1 + G_C V_{\text{IN}}). \tag{9}$$

Finally, the closed-loop output impedance, z_{out}, can be represented as [35], (10), as shown at the bottom of this page. Substituting the individual terms back into (5)

$$\frac{i_{\text{in}}}{i_o} = \left(\underbrace{D\frac{i_l}{v_o}}_{\text{T1}} + \underbrace{I_0\frac{d}{v_o}}_{\text{T2}}\right)\frac{v_o}{i_o} = -\left(D\frac{i_l}{v_o} + I_0\frac{d}{v_o}\right)z_{\text{out}}. \tag{11}$$

The compensator transfer function is converted from discrete to continuous domain using the bilinear transformation

$$G_C(s) = (\eta_{\text{ADC}} G_C(z) \eta_{\text{DPWM}})|_{z=\frac{1-sT/2}{1+sT/2}} \tag{12}$$

where $G_C(z)$ is the compensator transfer function in the discrete domain, η_{ADC} and η_{DPWM} are the small signal gain across the ADC and the DPWM, and T is the sample period.

The reversibility transfer function (RTF) from the IVR input current to the load current is the reciprocal of transfer function of (5). Fig. 22(a) shows the magnitude of different components of (5) and the RTF against frequency and the relevant pole-zero locations. $T2$ (11) has two zeroes defined by the compensator (complex zeroes at the same frequency due to discrete to continuous domain transformation). $T1$ has two zeros (compensator zeroes split apart due to the addition term of 1) and three poles (two due to the compensator poles and one due to the inductor ESR pair). The poles of z_{out} are due to the filter double pole. Overall, the RTF shows two zeroes near the output filter cutoff frequency, which amplifies the small signal gain beyond that frequency. This behavior compensates the attenuation in the forward transfer function due to the filter double poles.

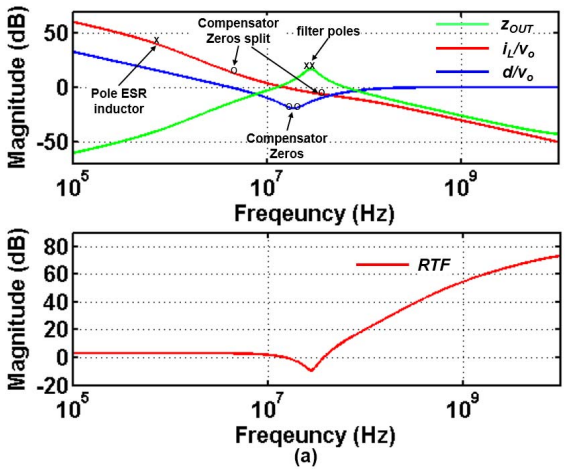

TABLE II
ATTACK USING RTF

IVR-AES Design Settings	Baseline	Zero Loc 1	Zero Loc 2	DCM	LR
Max t-val after RTF	3.53	2.28	3.73	3.60	3.14

(b)

Fig. 22. (a) Small signal transfer function of RTF and its components. (b) TVLA results after estimation using RTF.

2) Load Current Estimation Using RTF: To generate the estimated load current, the RTF can be used as a linear system with the measured IVR input current as an input to the system. However, for nonzero controller delay, RTF can have equal or more zeroes than poles, causing a linear simulation to fail. Hence, the following approach of computation through frequency domain is adopted. A window is selected from time domain signature of $V_{\text{IN,IVR}}$ and converted into FFT. Next, the magnitude of the RTF at the corresponding points of FFT is multiplied and the result is converted back to time domain through IFFT.

3) Results: The measured $V_{\text{IN,IVR}}$ signatures for a HP-AES and the estimated RTF are used to predict the corresponding load current signatures at the IVR output. It is assumed for the sake of the threat model that the attacker has complete knowledge of the pole-zero locations of the compensator and the RTF is modified accordingly. Although this approach works fine for the simulated input current signatures [19], no TVLA leakage was observed after applying RTF on the $V_{\text{IN,IVR}}$ signatures in the baseline-IVR configuration as well as with different zero locations, DCM mode and with LR ON, as given in Table II. One of the possible reasons can be the high frequency noise in a measured signature, is amplified after RTF and thereby reduces the correlation.

B. CPA Using Templates

Loop randomizer introduces a steady semi-random perturbation in the captured signatures. Filtering followed by alignment

$$z_{\text{out}} = \frac{R_O(sL + R_L)(1 + sCR_C)}{(1 + G_C(s)V_{IN})R_O(1 + sCR_C) + (sL + R_L)(1 + sC(R_C + R_O))} \tag{10}$$

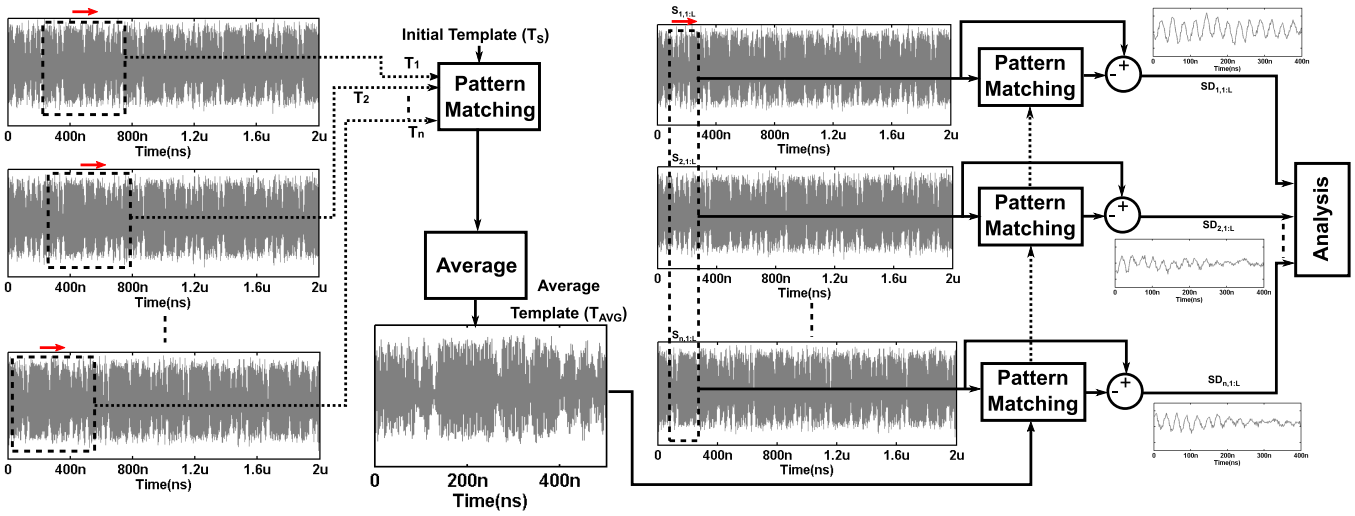

Fig. 23. CPA using template subtraction.

might fail to exploit the data-dependency of the signatures as the variation in the output voltage has pseudo-randomness due to the LR. Even if the same plaintext is encrypted multiple times, each signature will show a unique pattern at the point of interest. Therefore, the higher order attacks like template attack, mutual information analysis, which assume that the magnitude of the signatures are data dependent at a given time instant might also fail along with a CPA. Instead, we introduce a different attack, particularly when LR mode is enabled. The maximum length 4-bit LFSR which inserts delays proportional to the LFSR outputs into the IVR control loop, repeats the sequence after 15 combinations. The LFSR runs at 1/8th of the frequency of the digital controller (250 MHz), therefore, power signatures repeat at a frequency of ∼2 MHz as shown in Fig. 23. We propose to use an averaged power signature template of one iteration of the LFSR and perform the attack on the differential signal between the captured signature and the template.

The steps of the proposed attack are described in Fig. 23. The analysis has two components. In template construction part, a seed template (T_s) of length 0.5 μs is first chosen from a randomly selected trace. Next, for all the traces, templates of the same length ($T_i, 1 \leq i \leq n$) are obtained through pattern matching with T_s. The templates (T_i) are averaged to generate the final template (T_{avg}). In the attack part, a time window ($S_{i,1:L}, 1 \leq i \leq n$) of length L, smaller than the length of T_{avg} is selected for all the traces. Next, the differential signature ($\text{SD}_{i,1:L}$) is found according to the following equation:

$$\begin{aligned} P_{i,1:L} &= \text{PM}(T_{\text{avg}}, S_{i,1:L}), \quad 1 \leq i \leq n \\ \text{SD}_{i,1:L} &= S_{i,1:L} - P_{i,1:L}, \quad 1 \leq i \leq n \end{aligned} \tag{13}$$

where PM represents the pattern matching performed through cross correlation. $\text{SD}_{i,1:L}$ removes the effect of steady-state variations due to LR. Next, a CPA is performed on SD_i, $1 \leq i \leq n$ for different sliding time windows.

1) Results: We performed the aforementioned attack for both the HP-AES and the LP-AES with 500 000 traces of LR. No successful CPA was observed with 500 000 traces for each of the designs. This indicates that the protection is not achieved due to the addition of a randomized pattern at the captured signature, rather the interaction of the LR with the perturbation at the output voltage as well as the misalignment effect.

C. EM Attack

A frequently exploited side channel for encryption engines is electromagnetic radiation from the hardware platform [36]–[38]. The transformations of an inductive IVR are effective for PSCA protection as the point of observation is limited to the input of the IVR. However, an EM attack is typically carried out using EM probes which can be found in a wide variety of resolutions [38], [39] and the EM signature can be captured from multiple locations of the targeted hardware as the attack is non-invasive in nature. Therefore, an attacker has multiple knobs through which the measurement process can be improved. One simple technique to bypass the role of an inductive IVR or any other generic PSCA countermeasure which does not alter the architecture/logic/physical design of the encryption engine, would be to place the EM probe close to the physical location of the AES engine. Interestingly, due to the continuous switching of the power stage, the current through the inductor in an inductive IVR continuously changes in every cycle and emits a strong EM signature. As the form factor of the inductance is continuously shrinking due to superior integration [12], [40], separating out the inductor EM emission and the same from the AES engine becomes challenging. As the emission from the inductance is a direct function of the current flowing through it (I_L, in Fig. 2), which also happens to be a derived version of the IVR input current (I_{IN}); the current transformations through an IVR might be effective for protecting against EM attack as well.

1) CEMA Using a Passive Probe: We selected a passive EM probe of Beehive Corp. with a loop diameter of 0.4 in and a 50-Ω load. The probe is placed at the middle of the chip package [Fig. 24(a)]. Fig. 24(b) shows a sample EM waveform (time domain) and its corresponding spectrogram.

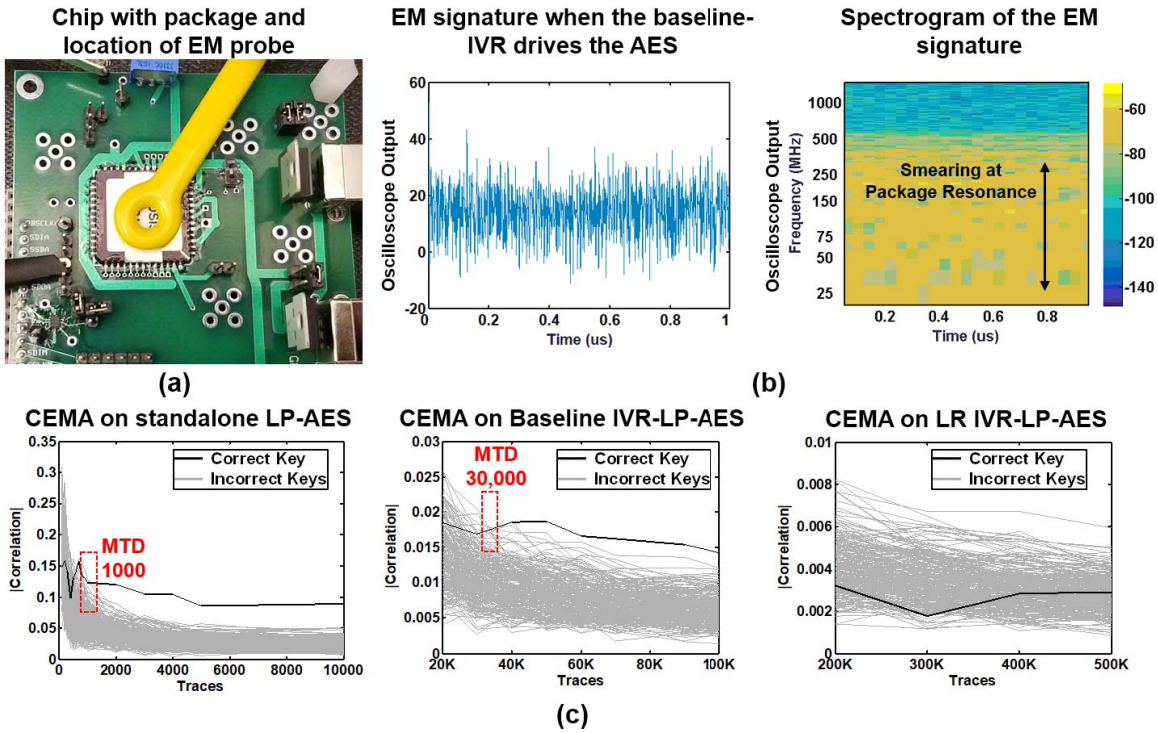

Fig. 24. (a) Measurement setup of EM analysis using a sample EM probe. (b) Captured waveform in time domain and spectrogram. (c) CEMA on the LP-AES in standalone, baseline-IVR, and LR-IVR mode.

The spectrogram shows a frequency smearing effect near the IVR switching frequency and its harmonics. Fig. 24(c) shows the results of correlation electromagnetic analysis (CEMA) using a Hamming weight power model on the LP-AES. Both the standalone AES and the baseline-IVR configurations were attacked with less than 100 000 traces. The MTD of the baseline-IVR configuration in CEMA (30 000) is 20× more than the MTD in CPA for the same configuration (1500). This is due to the spurious frequency components generated by the inductance. Enabling the LR mode successfully prevents a CEMA for 500 000 traces.

2) Discussion: The initial EM measurements with a specific type of probe are promising. However, to reach a conclusion on the effect of inductive IVRs on improving EM side-channel resistance, EM probes with different resolutions as well as different locations for signature capture are required. This paper, therefore, only demonstrates protection against power-based side channel attack and does not convincingly demonstrate the effect of IVR on EM side-channel leakage.

VI. Conclusion

Dedicated accelerators and instruction set for encryption are emerging as critical components of modern processors for high-performance as well as low-power platforms. Securing these systems against power side-channel attacks without a significant power/performance overhead is critical for the current and future processors. This paper demonstrated that inductive IVRs with security aware loop control can be exploited to improve PSCA resistance of AES engines. The proposed all-digital and synthesizable loop randomizer incurs only 3% overhead in the maximum operating frequency and significantly improves PSCA resistance of high-performance and serialized low-power architecture. Although, the initial EM measurements with a specific type of probe are promising, this paper does not provide any conclusion on the effect of IVR on EM side-channel leakage, and therefore, the future work needs to investigate the impact of inductive IVR for improving EM side-channel resistance.

References

[1] P. Hammarlund, "Haswell: The fourth-generation Intel core processor," *IEEE Micro*, vol. 34, no. 2, pp. 6–20, Mar./Apr. 2014.
[2] C. F. Webb, "IBM z10: The next-generation mainframe microprocessor," *IEEE Micro*, vol. 28, no. 2, pp. 19–29, Mar. 2008.
[3] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Advances in Cryptology—CRYPTO '99*. Springer, 1999, p. 789.
[4] M. Rivain and E. Prouff, "Provably secure higher-order masking of AES," in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst.*, Aug. 2010, pp. 413–427.
[5] J. A. Ambrose, S. Parameswaran, and A. Ignjatovic, "MUTE-AES: A multiprocessor architecture to prevent power analysis based side channel attack of the AES algorithm," in *Proc. IEEE/ACM Int. Conf. Comput.-Aided Design*, Nov. 2008, pp. 678–684.
[6] M. Nassar, S. Bhasin, J.-L. Danger, G. Duc, and S. Guilley, "BCDL: A high speed balanced DPL for FPGA with global precharge and no early evaluation," in *Proc. Conf. Design, Autom. Test Eur.*, 2010, pp. 849–854.
[7] M. Bucci, L. Giancane, R. Luzzi, and A. Trifiletti, "Three-phase dual-rail pre-charge logic," in *Cryptographic Hardware and Embedded Systems—CHES*, L. Goubin and M. Matsui, Eds. Berlin, Germany: Springer, 2006, pp. 232–241.
[8] 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.
[9] W. Xinmu *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.

[10] T. Guneysu and A. Moradi, *Generic Side-Channel Countermeasures for Reconfigurable Devices*. Berlin, Germany: Springer, 2011, pp. 33–48.
[11] H. K. Krishnamurthy *et al.*, "A 500 MHz, 68% efficient, fully on-die digitally controlled buck Voltage Regulator on 22nm Tri-Gate CMOS," in *Symp. VLSI Circuits Dig. Tech. Papers*, 2014, pp. 1–2.
[12] H. K. Krishnamurthy *et al.*, "A digitally controlled fully integrated voltage regulator with 3-D-TSV-based on-die solenoid inductor with a planar magnetic core for 3-D-stacked die applications in 14-nm Tri-Gate CMOS," *IEEE J. Solid-State Circuits*, vol. 53, no. 3, pp. 1038–1048, Apr. 2018.
[13] N. Sturcken *et al.*, "A 2.5D integrated voltage regulator using coupled-magnetic-core inductors on silicon interposer delivering 10.8A/mm^2," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, 2012 pp. 400–402.
[14] 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.
[15] 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.
[16] 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.
[17] 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.
[18] 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. (CICC)*, Sep. 2014, pp. 1–4.
[19] 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. ISLPED*, 2016, pp. 130–135.
[20] B. J. G. Goodwill, J. Jaffe, and P. Rohatgi, "A testing methodology for side-channel resistance validation," in *Proc. NIST Non-Invasive Attack Testing Workshop*, 2011, pp. 1–15.
[21] A. Satoh, S. Morioka, K. Takano, and S. Munetoh, "A compact Rijndael hardware architecture with S-BOX optimization," in *Proc. ASIACRYPT*, 2001, pp. 239–254.
[22] S. Mathew *et al.*, "340 mV–1.1 V, 289 Gbps/W, 2090-Gate NanoAES hardware accelerator with area-optimized encrypt/decrypt GF(2 4) 2 Polynomials in 22 nm Tri-Gate CMOS," *IEEE J. Solid-State Circuits*, vol. 50, no. 4, pp. 1048–1058, Apr. 015.
[23] M. Kar, A. Singh, A. Rajan, V. De, and S. Mukhopadhyay, "An all-digital fully integrated inductive buck regulator with a 250-MHz multi-sampled compensator and a lightweight auto-tuner in 130-nm CMOS," *IEEE J. Solid-State Circuits*, vol. 52, no. 7, pp. 1825–1835, Jul. 2017.
[24] Y. M. Tousi and E. Afshari, "A miniature 2 mW 4 bit 1.2 GS/s delay-line-based ADC in 65 nm CMOS," *IEEE J. Solid-State Circuits*, vol. 46, no. 10, pp. 2312–2325, Oct. 2011.
[25] T.-H. Le, J. Clédiére, C. Canovas, B. Robisson, C. Serviére, and J.-L. Lacoume, "A proposition for correlation power analysis enhancement," in *Cryptographic Hardware and Embedded Systems—CHES*, L. Goubin and M. Matsui, Eds. Berlin, Germany: Springer, 2006, pp. 174–186.
[26] M. Kar, A. Singh, S. Mathew, A. Rajan, V. De, and S. Mukhopadhyay, "8.1 improved power-side-channel-attack resistance of an AES-128 core via a security-aware integrated buck voltage regulator," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2017, pp. 142–143.
[27] 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. C246–C247.
[28] M. Doulcier-Verdier, J.-M. Dutertre, J. Fournier, J.-B. Rigaud, B. Robisson, and A. Tria, "A side-channel and fault-attack resistant AES circuit working on duplicated complemented values," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2011, pp. 274–276.
[29] M. T. Wich, "On-chip power supply interface with load-independent current demand," U.S. Patent 6 963 188 B2, Nov. 8, 2005,
[30] R. Mohel, A. Owsianko, A. Seloni, R. Dvash, and A. Yefet, "Device and method for preventing wiretapping through power supply lines," U.S. Patent 9 312 751 B2, Apr. 12. 2016.
[31] G. B. Ratanpal, R. D. Williams, and T. N. Blalock, "An on-chip signal suppression countermeasure to power analysis attacks," *IEEE Trans. Depend. Sec. Comput.*, vol. 1, no. 3, pp. 179–189, Jul. 2004.
[32] D. Das, S. Maity, S. B. Nasir, S. Ghosh, A. Raychowdhury, and S. Sen. (Mar. 2017). "High efficiency power side-channel attack immunity using noise injection in attenuated signature domain." [Online]. Available: https://arxiv.org/abs/1703.10328
[33] S.-K. Kim, "Smart cards having protection circuits therein that inhibit power analysis attacks and methods of operating same," Google Patents, U.S. Patent 7,620,823, Nov. 17, 2009.
[34] H. Hernandez, J. Scott, and W. Van Noije, "DPA insensitive voltage regulator for contact smart cards," in *Proc. 25th Symp. Integr. Circuits Syst. Design (SBCCI)*, Aug. 2012, pp. 1–4.
[35] K. Yao, Y. Meng, P. Xu, and F. C. Lee, "Design considerations for VRM transient response based on the output impedance," in *Proc. 17th Annu. IEEE Appl. Power Electron. Conf. Expo. (APEC)*, vol. 1. Jun. 2002, pp. 14–20.
[36] D. Genkin, L. Pachmanov, I. Pipman, and E. Tromer, "ECDH key-extraction via low-bandwidth electromagnetic attacks on PCs," in *Proc. Cryptographers' Track RSA Conf.*, 2016, pp. 219–235.
[37] D. Genkin, L. Pachmanov, I. Pipman, and E. Tromer, "Stealing keys from PCs using a radio: Cheap electromagnetic attacks on windowed exponentiation," in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst.*, 2015, pp. 207–228.
[38] T. Korak, T. Plos, and M. Hutter, "Attacking an AES-enabled NFC tag: Implications from design to a real-world scenario," in *Proc. Int. Workshop Construct. Side-Channel Anal. Secure Design*, 2012, pp. 17–32.
[39] J. Longo, E. De Mulder, D. Page, and M. Tunstall, "SoC it to EM: Electromagnetic side-channel attacks on a complex system-on-chip," in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst.*, 2015, pp. 620–640.
[40] N. Sturcken *et al.*, "Magnetic thin-film inductors for monolithic integration with CMOS," in *IEDM Tech. Dig.*, Dec. 2015, pp. 4–11.

Monodeep Kar (S'12–M'17) received the B.Tech. degree in electronics and electrical communication engineering from IIT, Kharagpur, India, in 2012, 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.

He is currently a Research Scientist in the Intel's Circuit Research Lab, Hillsboro, OR, USA. He has authored over 20 conference/journal papers. His current research interests include hardware security, power management in digital circuits, and hardware accelerators for high performance applications.

Arvind Singh (S'15) received the B.S. and M.S. degrees in electrical engineering from IIT, Kanpur, Kanpur, India, in 2010. He is currently pursuing the Ph.D. degree in electrical and computer engineering with the Georgia Institute of Technology, Atlanta, GA, USA, under the supervision of Prof. S. Mukhopdhyay.

From 2010 till 2014, he was with the ASIC Physical Design Team, NVIDIA, Bengaluru, India, where he was involved in tapeouts of multiple generations of Tegra mobile processors. He was an Intern with the Circuits Research Labs, Intel, Hillsoboro, OR, USA, and the ASIC/VLSI Research Group, Qualcomm, San Diego, CA, USA, in 2016 and 2017, respectively. His current research interests include hardware security, low-power design, and power management in digital circuits.

Sanu K. Mathew (M'99–SM'15–F'18) 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.

In 1999, he joined Intel Corporation. He is currently a Senior Principal Engineer with the Circuits Research Laboratories, Intel, Hillsboro, OR, USA, where he is responsible for developing energy-efficient security circuit primitives for next-generation microprocessors. He also mentors Intel and SRC-funded research projects in leading universities. He has authored or co-authored over 77 conference/journal papers. He holds 41 issued patents and 63 patents pending. His current research interests include high-speed/low-power computer arithmetic datapath circuits and special-purpose hardware accelerators for cryptography and security.

Dr. Mathew was a recipient of the ISSCC Distinguished Technical Paper Award in 2012. He has served on the program committees for the ARITH, ISLPED, DAC, and SOCC conferences.

Anand Rajan was the Technical Lead of the Trusted-UNIX Team, Sequent Computer Systems, where he was involved in the development and certification of a TCSEC B1-level Operating System. He joined Intel, Hillsboro, OR, USA, in 1994, where he is currently the Senior Director of the Emerging Security Laboratory. He leads a team of researchers, whose mission is to investigate novel security features that raise the assurance of platforms across the compute continuum (cloud to wearables). The topics covered by his team span trustworthy execution environments (TEE), Internet of Things (IoT) and mobile security, cryptography, and security for emerging paradigms, including autonomous systems and 5G. He is also a Principal Investigator for Intel's research collaboration with academia, government, and commercial laboratories on trustworthy platforms. He is the mentor for the Security Research Sector of Intel's Corporate Research Council. He and his team developed the common data security architecture specification that was adopted as a worldwide standard by The Open Group. His team was also instrumental on several security standardization efforts, such as PKCS#11, BioAPI, UPnP-Security, and EPID.

Dr. Anand was an Active Member of the IEEE Working Group that crafted the P1363 (public-key crypto) standard.

Vivek De (F'11) received the B.Tech. degree in electrical engineering from IIT Madras, Chennai, India, the M.S. degree in electrical engineering from Duke University, Durham, NC, USA, and the Ph.D. degree in electrical engineering from the Rensselaer Polytechnic Institute, Troy, NY, USA.

He is currently an Intel Fellow and the Director of Circuit Technology Research in Intel Labs. He is responsible for providing strategic technical directions for long term research in the future circuit technologies and leading energy efficiency research across the hardware stack. He has authored or co-authored over 270 publications in refereed international conferences and journals with a citation H-index of 73. He holds 220 patents issued with 30 more patents filed (pending).

Dr. De was a recipient of an Intel Achievement Award for his contributions to an integrated voltage regulator technology, the Best Paper Award at the 1996 IEEE International ASIC Conference, nominations for the Best Paper Awards at the 2007 IEEE/ACM Design Automation Conference (DAC), and the 2008 IEEE/ACM International Conference on Computer-Aided Design (ICCAD). He also co-authored a paper nominated for the Best Student Paper Award at the 2017 IEEE International Electron Devices Meeting (IEDM). One of his publications was recognized in the 2013 IEEE/ACM DAC as one of the Top 10 Cited Papers in 50 Years of DAC. Another one of his publications received the Most Frequently Cited Paper Award in the IEEE Symposium on Very Large Scale Integration (VLSI) Circuits at its 30th Anniversary in 2017. He was recognized as a Prolific Contributor to the IEEE International Solid-State Circuits Conference (ISSCC) at its 60th Anniversary in 2013, and a Top 10 Contributor to the IEEE Symposium on VLSI Circuits at its 30th Anniversary in 2017. He served as an IEEE/EDS Distinguished Lecturer in 2011 and an IEEE/SSCS Distinguished Lecturer in 2017–2018. He received the 2017 Distinguished Alumnus Award from the IIT Madras, Chennai, India.

Saibal Mukhopadhyay (S'99–M'07–SM'11–F'18) received the Ph.D. degree in electrical and computer engineering from Purdue University, West Lafayette, IN, USA, in 2006.

He is currently a Professor with the School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA, USA. He has authored or co-authored over 150 papers in refereed journals and conferences. He holds five U.S. patents. His current research interests include neuromorphic computing, low-power mixed-signal systems, voltage regulation, and power and thermal management.

Dr. Mukhopadhyay was a recipient of the Office of Naval Research Young Investigator Award in 2012, the National Science Foundation Career Award in 2011, the IBM Faculty Partnership Award in 2009 and 2010, the SRC Inventor Recognition Award in 2008, the SRC Technical Excellence Award in 2005, the IBM Ph.D. Fellowship Award in 2004 and 2005, and the Best Paper Awards in the IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS in 2014, the IEEE TRANSACTIONS ON COMPONENT, PACKAGING, AND MANUFACTURING TECHNOLOGY in 2014, and the IEEE/ACM International Symposium on Low-Power Electronic Design in 2014.