This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCAD.2022.3144369, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems

EM SCA White-box Analysis Based Reduced Leakage Cell Design and Pre-Silicon Evaluation

Debayan Das, Mayukh Nath, Baibhab Chatterjee, *Student Member, IEEE,*
Raghavan Kumar, Xiaosen Liu, Harish Krishnamurthy, Manoj Sastry, *Senior Member, IEEE,*
Sanu Mathew, *Fellow, IEEE,* Santosh Ghosh, Shreyas Sen, *Senior Member, IEEE*

***Abstract*—This work presents a white box modeling of the electromagnetic (EM) leakage from an integrated circuit (IC) to develop EM side-channel analysis (SCA) aware design techniques. A new digital library cell layout design technique is proposed to minimize the EM leakage and is evaluated using a high frequency structure simulator (HFSS)-based framework. Backed by our physics-based understanding of EM radiation, the proposed double-row power grid based digital cell layout design shows $> 5\times$ reduction in the EM SCA leakage compared to the traditional digital logic gate layout design. Further, exploiting the magneto-quasistatic (MQS) regime of operation of the EM leakage from the CMOS circuits, the HFSS-based framework is utilized to develop a pre-silicon (Si) EM SCA evaluation technique to assess the vulnerability of cryptographic implementations against such attacks during the design phase itself.**

***Index Terms*—EM Side-channel attack, white-box modeling, logic gate layout design, power grid, pre-silicon EM SCA evaluation.**

I. Introduction

THE increasing demand of internet-connected and miniaturized devices calls for stringent security requirements which has led to the development of robust and mathematically-secure cryptographic algorithms like AES, SHA, RSA. These classical cryptographic algorithms are responsible for providing confidentiality, integrity, and authenticity in critical platform features like secure boot, trusted platform module (TPM), secure debug, and so on, and hence they are designed to be highly resilient against probabilistic polynomial time (PPT) attackers. However, over the last two decades, many of these algorithms have been broken by taking advantage of its underlying physical implementation to recover secret parameters like the encryption key utilizing what is known as side-channel analysis (SCA) [1]. In this work, we focus on electromagnetic (EM) SCA attacks, which is a non-invasive attack on embedded electronic devices to recover the secret key [2], [3].

A. Motivation

Recently, it was shown that the AES-256 encryption key could be broken in just five minutes from a distance of 1 meter [4]. Most commercial devices today are transitioning from AES-128 to AES-256 for encryption to provide enhanced data security. Although AES-256 provides exponential improvement in the computational security compared to AES-128, the side-channel security only increases linearly [5], [6]. Several practical side-channel attacks using simple/differential/correlational EM analysis (SEMA/DEMA/CEMA) [2], [3], on crypto devices have been demonstrated over the recent years. Moreover, the continuous advancement of the low-cost high-resolution EM probes is increasing the threat surface of the embedded devices significantly. Hence, it becomes extremely imperative to protect against these EM SCA attacks.

Most prior works on EM SCA countermeasures treat the crypto engine as a black box without analyzing the root-cause of the EM leakage. Hence, the solutions typically involve high overheads in terms of performance, power, and area. This work treats the cryptographic hardware as a white-box and proposes EM leakage reduction techniques during the design phase itself. In our recent works, it has been shown that the root-cause of the EM leakage from the crypto hardware implementation depends significantly on the higher-level metal

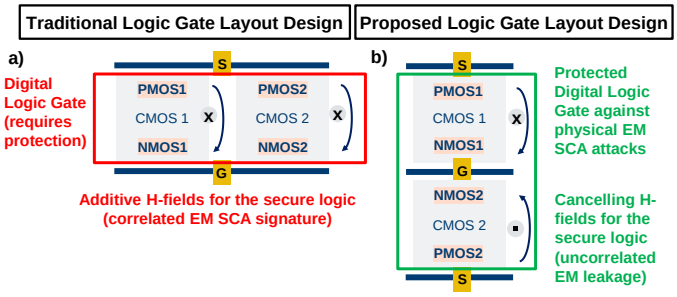

Fig. 1: Key concept: (a) The conventional digital library logic cells are routed in the same row of the power grid (between supply (S) and ground (G) rails), and hence the current flow for the switching events are in the same direction, resulting in additive magnetic (H) fields, whereas, (b) the proposed digital library cell with the layout design split across two power grid rows (S, G, S) results in opposing currents in the alternating cell rows leading to cancellation in the H-field (which tends to be the dominant contributor to the EM leakage due to the formation of current loops in ICs [7], [8]), thereby minimizing the EM leakage significantly at the gate-level itself. This paper builds a framework to analyze this key idea and extends this framework towards pre-silicon (Si) EM SCA evaluation.

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

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

R. Kumar, X. Liu, H. Krishnamurthy, M. Sastry, S. Mathew, S. Ghosh are with Intel Labs, Hillsboro, OR, 97124 USA.

layers as they behave as more efficient antennas [9], [10]. In this work, we deep-dive into the individual logic gate designs and investigate their layouts to provide insightful and intuitive design guidelines to minimize the EM radiation.

Moreover, it should be noted that, till now, most of the EM analysis and evaluation of a countermeasure is performed only after the chip has been fabricated, that is, in the post-silicon (Si) phase, since the EM leakage could not be measured without the physical chip. Only a few recent works exist on developing a pre-Si EM SCA evaluation framework [7], [11], [12]. The framework used in [11] is based on extracting the circuit currents from Virtuoso and then using a custom-built framework for EM analysis through a theoretical modeling, which has not been validated through measurements. [7], [12] have used Redhawk which is a static IR-drop simulator followed by a custom-built framework for H-field approximation. These custom-built frameworks are not easily reproducible and hence we want to utilize the existing commercial EM analysis tools like the Ansys HFSS. However, HFSS in itself cannot simulate an entire crypto circuit because of the high complexity of the layout and the small geometries involved. Our goal is to exploit the MQS nature of the EM leakage from a crypto IC along with the white-box understanding of the EM leakage to optimally utilize commercial frameworks like HFSS (along with Virtuoso for the current extraction) which provides an accurate prediction of the EM SCA leakage from a crypto IC. Hence, in this work, we utilize the HFSS-based framework developed for our white-box modeling to evaluate the resilience of the crypto implementations against EM SCA attacks prior to the fabrication, that is, in the pre-Si phase.

Overall, this work aims to provide EM SCA aware design strategies to protect against these EM attacks, develops a framework for the ground-up root-cause analysis, and simultaneously proposes to leverage this framework towards pre-Si EM SCA evaluation.

B. Contribution

The key contributions of this work are:

- Utilizing physics-level understanding of the near-field radiation from magnetic dipoles, the effect of the digital cell layout and the power grid is analyzed to provide insightful guidelines to the designer during the design phase itself prior to fabrication. Contrary to the conventional single-row layout of the standard digital library cells, we propose a double-row split-layout architecture across two rows of the power grid, showing a $> 5\times$ improvement in the radiated H-field (Section III, IV).
- An EM leakage evaluation framework for actual circuit layouts is developed using high frequency structure simulator (HFSS) by emulating the transistor switching events intelligently (using parameterized resistors) (Section III).
- Exploiting the MQS regime of the EM leakage from crypto circuits (given its frequency of operation and the geometry of the metal layers), the proposed framework can be leveraged towards evaluating the EM SCA attack resilience of crypto implementations in the pre-Si phase, thereby reducing the time-to-market significantly (Section V).
- The key concepts - EM SCA resilient design techniques through ground-up understanding and the pre-Si EM SCA evaluation are proven across two different processes (TSMC 65nm, Intel 10nm) and across two different set-ups (Purdue University, Intel Labs) (Section III-V).

C. Paper Organization

The remainder of the paper is organized as follows. Section II summarizes the prior state-of-the-art on EM SCA countermeasures. In Section III, the white-box modeling of the EM leakage using HFSS is introduced and the contribution of the EM leakage from the different layout patterns of the digital gates are analyzed. Section IV presents the results for the power grid analysis on the EM leakage using the proposed framework. In Section V, the HFSS-based framework is utilized to evaluate the pre-Si EM SCA attack resilience. Finally, Section VI concludes the paper.

II. Related Work

Over the last two decades, there have been significant advances in EM SCA, both in attacks as well as countermeasures. Many real-world attacks have been demonstrated on embedded devices to recover the secret key from its bootloader [13], [14]. Recently, SCA attacks have been demonstrated on bitcoin wallets to obtain the secret key of the device. In 2018, screaming side-channel was demonstrated, showing how the radio transmitter could radiate sensitive information regarding the digital logic on the same IC, leading to the recovery of the encryption key from a distance of up to 10 meters [15]. Fully-automated EM SCA attack framework (SCNIFFER) using gradient-search algorithm to detect high-leakage location on the target device have been proposed to accelerate these attacks [16]. In 2021, EM SCA attacks have been successfully performed on the iPhone devices to extract the hardware AES-256 secret key [17], as well as on the Google Titan security key [18]. Moreover, the recent advancements in machine-learning (ML) based profiled SCA attacks have been shown to break various crypto implementations in much fewer traces compared to the conventional CEMA/DEMA-based non-profiled SCA attacks [19]–[21].

Consequently, various solutions to prevent EM and power SCA have been proposed, which can be broadly classified into three categories - architectural, logical, and circuit-level (physical). Architectural countermeasures include shuffling [22], random insertion of dummy operations, software masking, and data path obfuscation [23]. Logical countermeasures include sense amplifier based logic (SABL), wave dynamic differential logic (WDDL), and gate-level masking [24]. Circuit-level countermeasures include digital low-dropout (LDO) regulators [25], [26], switched capacitors [27], and signature attenuation [28], [29]. Most of these solutions are algorithm-specific and incur high area/power overheads. We need a low overhead generic countermeasure to prevent EM SCA attacks. Hence, a white-box analysis is critical to understand the source of the EM leakage from an integrated circuit (IC).

Recently, in 2019, a root-cause analysis of the EM leakage from crypto ICs was performed which revealed that the higher

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCAD.2022.3144369, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems

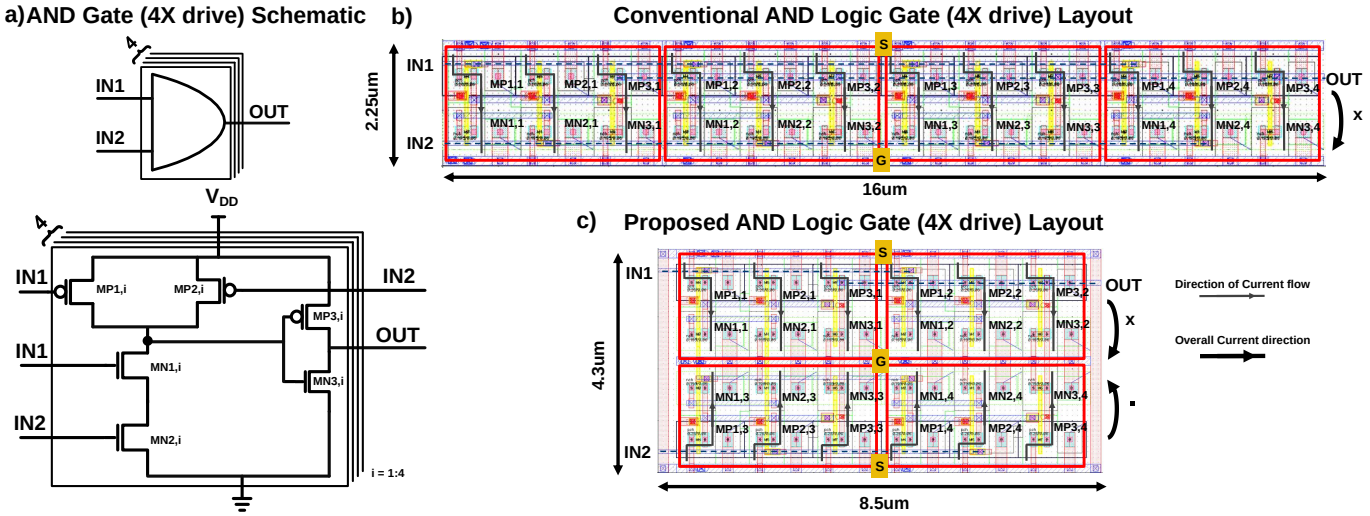

Fig. 2: Different layout patterns of the same AND logic gate circuit under analysis: (a) Schematic of the AND logic gate with 4X drive strength, (b) single-row power grid (SG), which is the conventional cell layout, and (b) proposed double-row power grid (SGS). Both the layouts for the AND gate circuit have the same areas, and the key difference in the proposed double-row power grid (SGS) is that the transistors placed in alternate rows are flipped in contrast to the conventional digital cell structure. However, negligible overheads are incurred by adopting the SGS power grid in place of the SG for the library cells (analyzed in Section IV. B), and it remains agnostic of the circuit under analysis (generic to any crypto core).

level metals are the main source of this radiation [5], [9]. Henceforth, signature attenuation with lower-metal routing was demonstrated to prevent EM SCA attacks for any crypto algorithm [5], [9]. This work extends the white-box modeling for real IC layouts and proposes layout modifications for the basic digital gates which would fundamentally provide more security benefits with minimal power/area overheads and without any performance overhead, and agnostic of any crypto algorithm.

Such white-box analysis calls for an in-depth understanding of the EM generation on-chip, which when incorporated as a part of the design process could aid in the identification of the vulnerabilities in the pre-Si phase itself. Notably, most of these previous works evaluate the EM SCA in post-Si after the chip is fabricated. Previous works on modeling this EM leakage from an IC have used EM analysis tools like Redhawk for the static IR-drop simulation followed by an analytical modeling using Biot Savart's law to obtain the magnetic field heatmap for an IC [7], [12]. [7] showed a validation of the modeling by incorporating noise in the framework. Another recent work [11] uses transient analysis to obtain the transient currents from Virtuoso, but it requires extracting the current information from thousands of branches which is extremely tedious to perform manually. Once the currents are obtained, the geometry information is extracted from the parasitics and then an analytical modeling is performed using the Maxwell's equations. Both these works [11], [12] have used theoretical equations to model the EM leakage without the use of commercially-validated tools to reduce complexity. Moreover, a static IR-drop based approach does not emulate the transient switching behavior of the transistors, and hence the electric (E)-field & magnetic (H)-field signatures in an IC. Further, none of the prior works have validated these custom-built models with commercial 3D Finite element method (FEM) simulators like Ansys HFSS. However, the main challenge is that HFSS cannot directly simulate an entire integrated circuit layout due to the high complexity of metal structures and the requirement of extensive graphics support. Even if it is able to simulate a full small circuit, it would take much longer than the prior works based on custom-built models. Recently, DARPA Side Channel Attack Testbench Estimator (SCATE) program has called for such pre-Si SCA evaluation framework development that can be performed in 24 hours. Keeping this in mind and utilizing the key insights from our physics-based white-box understanding and the MQS nature of the EM leakage, we develop a pre-Si EM SCA framework using the commercial tools (Virtuoso + HFSS) to make simulations feasible and faster.

Hence, in this work, along with the white-box analysis to develop EM SCA aware design techniques for the digital logic gates, we utilize the proposed HFSS-based framework towards building a pre-Si EM SCA evaluation technique that would be useful in analyzing the resiliency of crypto algorithms, as well as countermeasures, prior to the chip fabrication.

III. White-Box Modeling & Framework for the EM Leakage Analysis

In this section, we will discuss the white-box modeling of the EM leakage from an IC and explore design techniques to counter EM SCA.

This paper focuses on H-field analysis instead of E-field since the formation of current loops on an IC (forming H-field) is much more prominent than the effect of metal layer surfaces (creating E-field) [8]. This is corroborated by many of the prior works [7], [11], [12], which have thus focused on H-field analysis as well. Also, the operating frequencies of the CMOS

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCAD.2022.3144369, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems

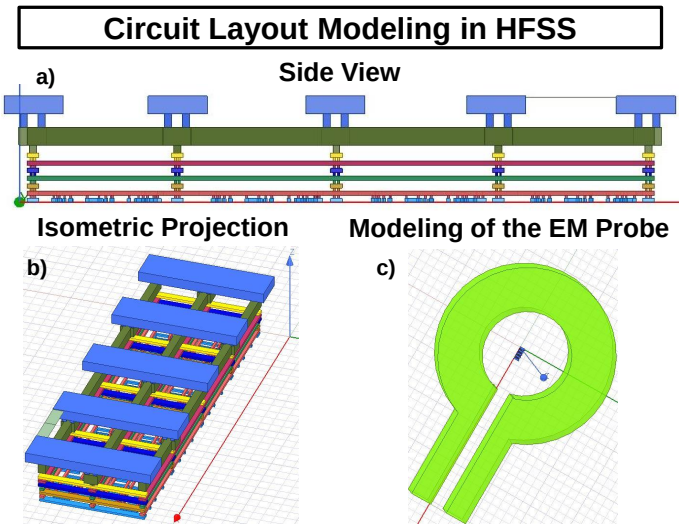

Fig. 3: HFSS modeling: (a) side-view of a layout design, imported to and modeled in HFSS with the parameterized resistors at the bottom layer, and the voltage excitation at the top layer, (b) isometric projection of the circuit layout, (c) modeling the EM probe ($100\mu m$ loop diameter) to estimate the amount of field received across the probe at a distance of $100\mu m$ on top of the circuit under analysis (mimicking an attacker) .

circuits have been limited to $< 10GHz$ primarily due to the power density limits, leading to the thermal density limits, and hence the frequency scaling in a core is restricted, moving towards multi-core designs over the last couple of decades. Hence, as we will prove later using simulations (Sec. V.C), at the operating frequencies of the CMOS circuits ($< 10GHz$), and the geometries of the metal layers involved (in μm range), the EM leakage from the circuits are in the MQS regime, which means that the EM radiation can be pre-dominantly approximated as H-field.

A. Reduced EM Leakage Cell Layout Design: Key Concept

Fig. 1(a, b) shows the key concept of the proposed digital gate layout design technique to minimize the EM leakage from an IC. Fig. 1(a) shows the conventional logic gate layout design which is typically seen today in the digital libraries, where the cells are placed in the same row of the power grid. Note that the same direction of current flow for all the transistors of the AND gate creates additive H-field, leading towards higher correlated EM leakage that can be picked up by an attacker.

Now, if we can somehow manage to cancel out the current flow such that the H-field is added destructively, we can minimize the EM SCA leakage picked up by an attacker. Fig. 1(b) shows the proposed logic gate design with the cells split across two rows of the power grid such that the alternating cell rows lead to canceling H-fields thereby minimizing the EM leakage from the source itself. As shown in Fig. 1, for the single-row power grid configuration, the current flow through the metal layers results in an additive H-field, while for the split double-row power grid digital gate design, the current flow results in opposing H-fields, leading to reduced EM leakage. As seen from Fig. 1(b), if the switching of one transistor generates a clockwise current, the transistor in the adjacent row would generate an anti-clockwise current, leading to the cancellation in the H-field.

Note that for the proposed power grid configuration of the digital cells, the transistors need to be flipped in the alternate rows. This feature can be readily accommodated by today's automatic place and route (APR) tools. Fig. 2(a) shows the proof-of-concept AND logic gate circuit with 4X drive strength with 6 transistors. Fig. 2(b, c) shows the actual layout of the AND gate circuit in TSMC 65nm process in SG (supply-ground, single row) and SGS (supply-ground-supply, double row) configurations respectively. The inputs (IN1, IN2) and the output (OUT) of the AND gate are marked as shown in Fig. 2(a, b, c). The current flow path for the conventional AND gate (Fig. 2(b, c)) is marked in light black, and the overall current flow is shown with dark black lines. In Fig. 2(c), for the SGS pattern, we can observe that the transistors in the two rows are flipped vertically, which ensures that the EM fields are cancelled out, in contrast to the single-row power grid layout where the EM fields get added constructively.

It is worth mentioning that, although the proposed double-row power grid layout technique does not incur any extra overheads, the only constraint it imposes is that the minimum size of the logic gates for the security-sensitive library has to be at least 2X (in our example, 4X is shown). The overhead analysis for the odd drive-strength gates are presented in the next section.

B. HFSS Modeling for EM Leakage Analysis

In the previous section, we proposed a double-row power grid based cell layout for minimizing the EM leakage. In this section, we will quantitatively analyze the impact of the proposed digital cell layout on the EM leakage.

Let us now investigate the EM leakage contribution from these different power grid structures implementing the same digital logic circuit with iso-area. For modeling the EM leakage from a circuit, first, we import the entire layout in HFSS and then provide the voltage excitation at the topmost metal layer (Fig. 3(a, b)) to emulate the powering of the chip during post-Si testing. Next, to emulate the transient currents during switching of the transistors, we insert parameterized resistors between the source and drain of the transistors. Making the parameterized resistor low resistance (short) emulates an ON transistor during the dynamic switching. Depending on the number of transistors switching at any given time, the EM leakage from the structure needs to be measured. In the later section (Sec. V), we show that only a few transistors need to be shorted, instead of all, to evaluate the EM leakage from the circuit.

Next, to analyze and compare the amount of EM leakage caused by the two different power grid layout structures, a commercially-available EM probe (Langer ICR HH100-27) with an $100\mu m$ probe loop diameter is modeled, as shown in Fig. 3(c). The EM probe is placed on top of the circuit

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCAD.2022.3144369, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems

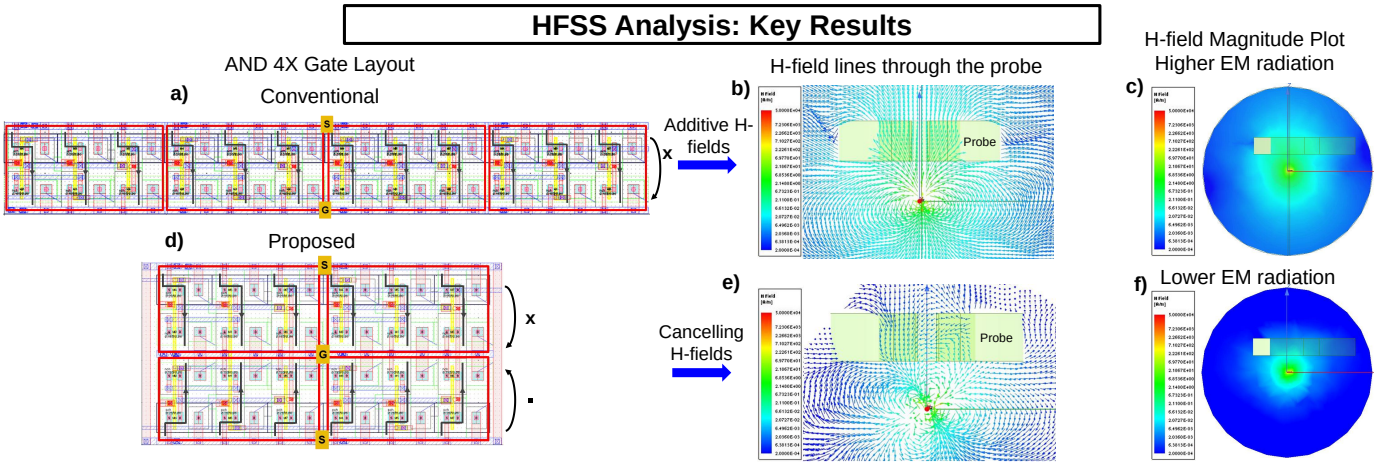

Fig. 4: HFSS Analysis of the AND circuit for the single-row (conventional) and double-row (proposed SGS power grid): (a) conventional single-row power grid layout, (b) H-fields get added constructively and passes through the EM probe, (c) showing high EM leakage. On the other hand, (d) for the proposed double-row (SGS) power grid pattern, (e) the fields cancel out, and (f) the EM radiation is reduced drastically.

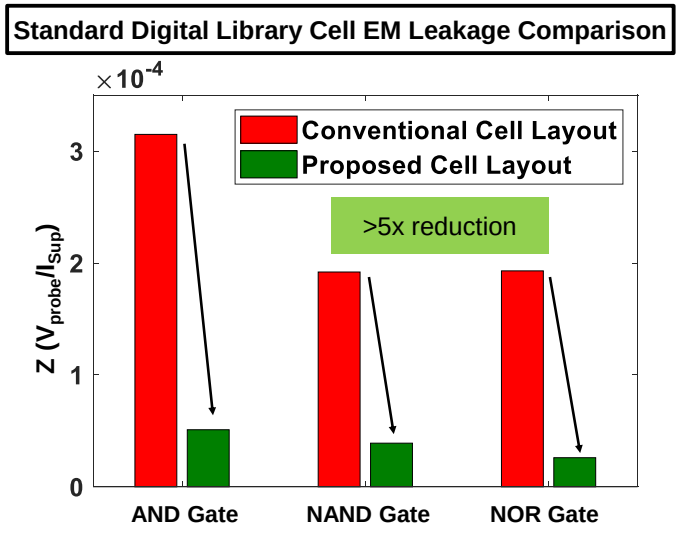

Fig. 5: Comparison of the digital cell layout design: The y-axis shows the ratio (Z) of the voltage induced across the EM probe (V_{probe}) and the current drawn from the supply (I_{sup}). The proposed double-row SGS power grid-based layout shows $> 5\times$ reduction in the EM leakage, compared to the traditional single-row power grid-based layout across multiple different logic gates (AND, NAND, NOR) circuit analyzed.

layout at a height of $100\mu m$ to capture the EM radiation from the switching events occurring in the circuit. From the HFSS framework, for the amount of current flow through the circuit (I_{sup}) depending on the number of transistors shorted at any given time, we obtain the power to EM mapping (Z), which is the ratio between the voltage received across the probe (V_{probe}) and the current drawn from the voltage source (I_{sup}).

Using this white-box modeling framework, in the next section, we will discuss the results and the effect of the different power grid configurations on the EM leakage.

IV. Results & Overhead Analysis: Effect of the Split Double-row Digital Cell Layout Design on the EM Leakage

A. Results

The two iso-area layout designs (single-row SG, double-row SGS) of the same AND logic circuit ((Fig. 4(a, d)) are analyzed using the HFSS-based framework. Fig. 4(b, e) shows the H-field vector plots for the single-row SG and the double-row SGS configurations respectively, and Fig. 4(c, f) shows the H-field magnitude plots for the same. For the single-row (SG) digital gate layout, the field lines pass vertically through the H-probe loop (revealing an additive superposition of the field lines) and hence produces a much higher EM leakage (Fig. 4(b, c), light blue). On the other hand, for the proposed double-row SGS layout structure, the EM field lines cancel out as discussed in the previous section, leading to horizontal field lines which do not pass through the EM probe (Fig. 4(e)), leading to significantly lower EM radiation (Fig. 4(e, f), dark blue) compared to the traditional single-row configuration, as seen from Fig. 4(c, f).

To quantitatively analyze the effect of the proposed double-row power grid structure for the digital gates, the power to EM mapping or the transfer function (Z) is computed, as discussed in Sec. IV. In comparison to the conventional single-row gate layout (SG), the double-row SGS power grid provides $> 5x$ reduction in the voltage induced across the EM probe for the same amount of switching activities across all the circuits analyzed (AND, NAND, as well as NOR gates), as shown in Fig. 5.

Fig. 6 shows the effect of the proposed layout structure on a 16:8 MUX circuit in presence of all the metal layers (M1-M9) for the TSMC 65nm technology. We observe that for the proposed double-row power grid layout, there is a $\sim 4\times$ reduction in the EM leakage compared to the traditional layout even in presence of all the higher metal layers. Note that the effective cancellation is slightly lower than the individual cells

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCAD.2022.3144369, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems

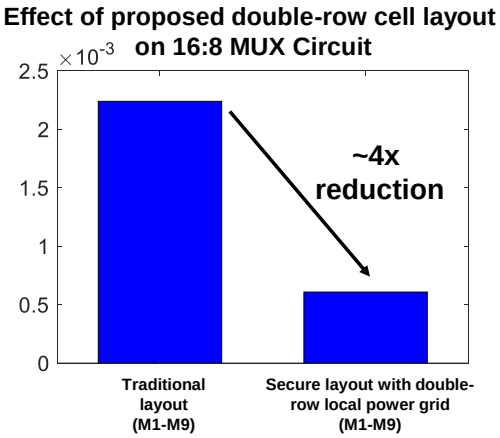

Fig. 6: Effect of the proposed split double-row power grid based cell layout on the 16:8 MUX circuit.

(Fig. 5) since the higher metal routing may not completely cancel out the global EM leakage. To cancel the global EM leakage fully, multi-pole routing can be used in the higher metal layers [8]. This is discussed in detail in Section V.F.

Fig. 7(a, b) shows an extended practical use case scenario of our proposed design technique for a full-chip layout. The idea is to use the double-row split layout architecture for the critical digital gates so that the overall correlated EM leakage is greatly minimized from the source itself. However, we do not need to minimize the leakage from other uncorrelated blocks/digital cells. Hence, as shown in Fig. 7(b), we propose using the existing standard digital library cells for the unrelated digital logic (other than crypto) and the double-row modified digital cell layout designs for the correlated critical digital gates to minimize the signature/signal-to-noise ratio (SNR). Further, this technique can be utilized to design the global power grid and cancel out the EM leakage even in the top metal layers.

B. Overhead Analysis

Table I summarizes the worst-case area, power, and performance overheads for the proposed countermeasure. Note that, for the double-row power grid layout, the drive strength must be even, which means that for an odd (n-X) drive-strength gates, the area overhead is $(\frac{n+1}{n} - 1) * 100\% = \frac{1}{n} * 100\%$, where n is odd. For even drive strength gates, however, there are no area overheads. Similarly, the power overhead for even drive strength gates will be zero. Now, for the power overhead of odd drive strength gates, it will depend on its load capacitance, which comprises of the self-loading capacitance, the interconnect capacitance, and the next stage capacitance. The self-loading capacitance will increase by a factor of $\frac{n+1}{n}$, while the interconnect capacitance and the next stage load capacitance remains the same. Considering the worst-case scenario when the self-loading capacitance dominates the overall load capacitance, the power overhead then becomes $\frac{1}{n} * 100\%$ for the n-X drive strength logic gate, when n is odd. Now, since the countermeasure is just a layout modification technique, it does not incur any performance overhead. Thus,

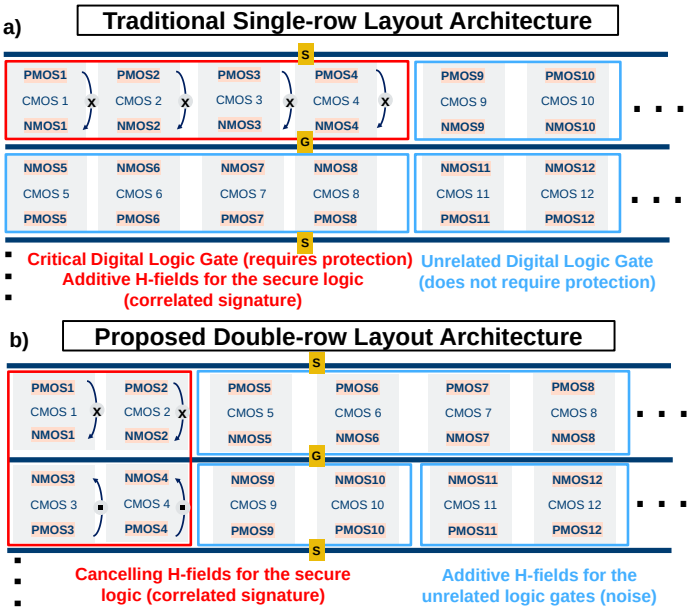

Fig. 7: (a, b) Practical use case of the proposed digital cell layout architecture for a full-chip layout. The proposed double-row power grid layout cell should be used for the security-critical digital logic to reduce the correlated EM leakage, while the traditional single-row gate layouts are used for unrelated logic (other than crypto), which do not require side-channel protection to enhance the uncorrelated EM leakage (increase system noise), so that the signal-to-noise ratio (SNR) of the EM measurements is reduced drastically for an attacker.

TABLE I: Overhead Analysis of the proposed technique

Overheads	%
Area	$\frac{1}{n} * 100$ [a]
Power	$\frac{1}{n} * 100$ [a]
Performance	~0 [b]

[a] Generalized for a n-X drive strength logic gate (only for odd n), else 0 for even n
[b] No performance overhead since the solution only re-organizes the layout

the proposed concept of double-row power grid layout is generic and can be applied to any crypto core with minimal area and power overheads and without any timing/performance overheads.

C. Discussion & Remarks

The supply-ground-supply (SGS) layout pattern for flipped cell routing is already supported by most of the commercially available automatic place and route (APR) tools. The proposed double-row power grid cells need to be added as a separate library for secure logic. This is analogous to the high threshold voltage (V_t) gates (like standard high V_t NAND gate), or even non-standard custom-built power gates, which form a separate library and can be recognized by the automatic place and route (APR) tool during layout.

Ideally, all the logic gates should be designed for the secure library to ensure high EM SCA security. Alternatively, we can

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCAD.2022.3144369, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems

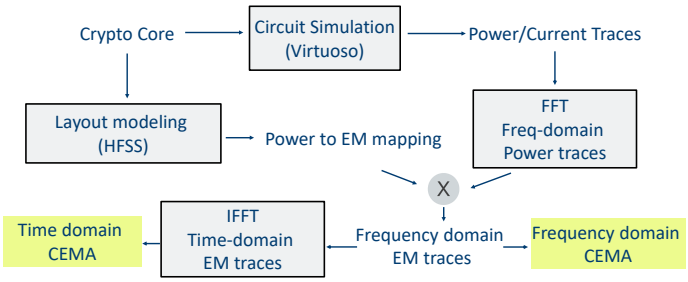

Fig. 8: Flowchart of the pre-Si EM SCA evaluation framework.

determine the leaky logic cells utilizing some of the recent prior works [30], [31], and only design the corresponding logic gates for the secure library following the proposed double-row power grid technique to enhance the side-channel security of the system.

The proposed double-row power grid based layout technique may seem somewhat similar to the wave dynamic differential logic (WDDL) based countermeasure [32] or to the design of twisted bit lines in memory arrays. WDDL is a current cancellation technique which in turn also cancels EM leakage. However, since it is primarily a current cancellation technique, WDDL incurs more than $2\times$ power and area overheads [32]. On the other hand, the proposed split double-row power grid technique is a direct EM cancellation technique without any additional current requirement.

For memory arrays, a twisted/folded bit line architecture is used to reduce the parasitic capacitance and hence less noise caused by the capacitive coupling (common mode noise rejection for the next stage differential sense amplifier circuit) among the bit line pairs during a sensing operation [33]. Hence, it is a capacitance cancellation technique, whereas our proposed method is an EM cancellation technique.

In the next section, we will explore how our proposed framework can be extended to be used for pre-Si EM SCA evaluation prior to fabrication.

V. HFSS-Based Pre-Silicon EM Side-channel Evaluation

Today, the EM SCA evaluation of a crypto algorithm is mostly performed after fabrication of the chip, that is, at the post-Si phase. Hence, the countermeasures developed cannot be pro-actively tested during the design life-cycle and the designers need to wait until the chip gets fabricated, which could cost a huge amount of time and money. Hence, having a framework for evaluating the crypto implementations before fabrication is extremely critical for a faster time-to-market from an industry viewpoint. In this section, we will extend our proposed framework for the white-box analysis towards incorporating a pro-active pre-Si EM SCA evaluation within the design life-cycle of crypto ICs.

A. Limitations of the existing commercial tools

Currently, commercial tools like Cadence Virtuoso allow us to perform pre-Si power SCA evaluation. Using circuit simulators like Virtuoso, post-layout current/power traces can be

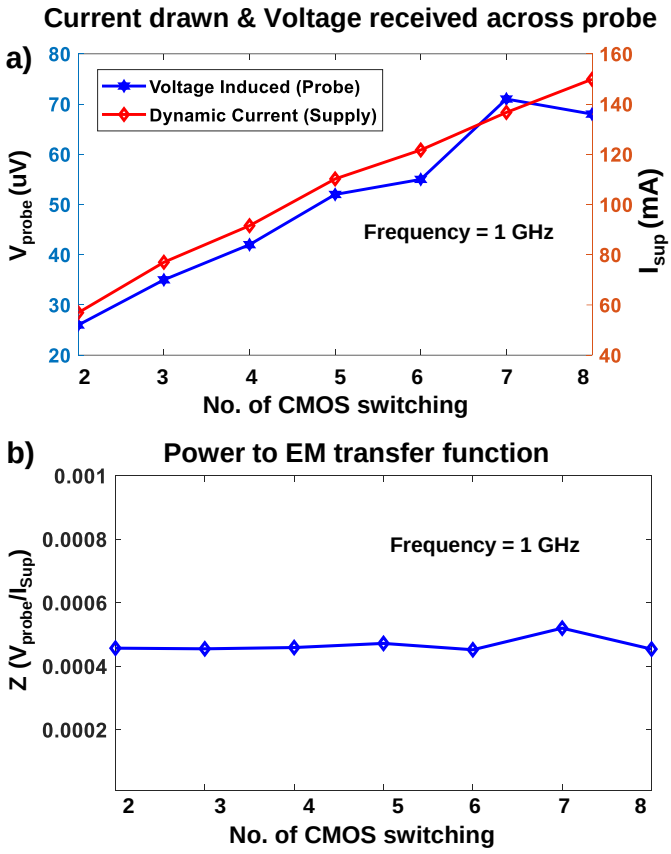

Fig. 9: Power to EM mapping: (a) The voltage induced across the EM probe (V_{probe}) and the current drawn from the supply (I_{sup}) for different number of CMOS switching events for a 16:8 MUX circuit is analyzed as a proof-of-concept. (b) The power to EM mapping/transfer function (Z) is independent of the number of switching events in the circuit.

extracted, but electric or magnetic fields cannot be estimated. On the other hand, Ansys HFSS and Redhawk (static IR-drop simulator) are used for EM analysis, and are popularly utilized for inductor or antenna design. However, HFSS or Redhawk cannot be used to simulate an entire circuit layout as it involves huge complexity. In this work, by identifying what precisely needs to be simulated in HFSS (unlike the prior works [11], [12]), we combine both the commercially-validated tools, Virtuoso and HFSS together, to obtain the EM traces and perform the pre-silicon EM side-channel analysis on any crypto algorithm (Fig. 8).

B. EM SCA Pre-Si Evaluation Framework: Key Concept

As shown in Fig. 8, the first step in building this framework for pre-Si EM SCA evaluation is to obtain the simulated post-layout current/power traces. Secondly, the layout of the circuit is modeled in HFSS and the power to EM mapping (Z) is obtained (Sec. III), specific to the circuit layout, across different frequencies. Thirdly, the time-domain power traces are transformed into the frequency-domain through fast fourier transform (FFT). This transformation to the frequency domain is performed for our convenience as we shall see in

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCAD.2022.3144369, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems

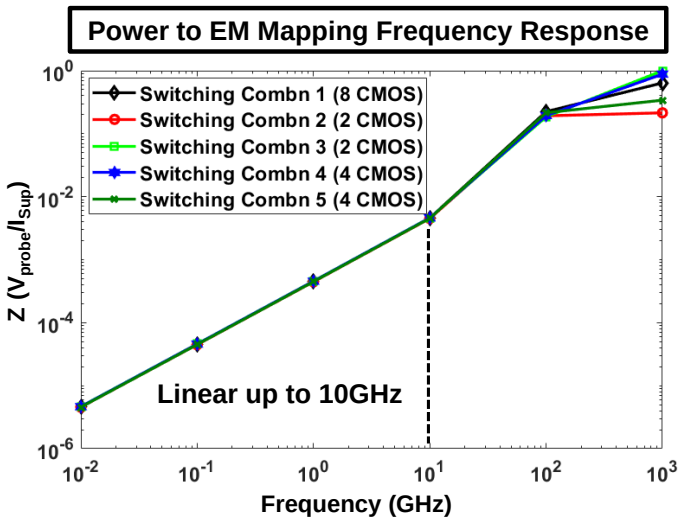

Fig. 10: Power to EM transfer function (Z) frequency response: Z remains linear with frequency up to $\sim 10GHz$, revealing the MQS mode of operation. Also, for the different transistor switching combinations, the mapping remains the same (as we see the curves are overlapping till $\sim 100GHz$).

the next sub-section. Now, this power to EM mapping is applied on the frequency-domain current traces to compute the corresponding frequency-domain EM traces (refer to Fig. 8). Finally, a frequency-domain CEMA is performed on the synthesized frequency-domain EM traces. Alternatively, the frequency-domain EM traces could also be transformed into time-domain and then the conventional time-domain CEMA can be performed to extract the secret key and evaluate the resiliency of the crypto system in the pre-Si environment.

C. Power to EM Transfer function & Frequency response

The power to EM transfer function (Z) for a 16:8 MUX circuit is shown in Fig. 9(a, b) as a proof-of-concept. Fig. 9(a) shows the voltage induced across the EM probe (V_{probe}) and the current drawn from the supply (I_{sup}) as a function of the number of transistors switching in the circuit. Fig. 9(b) shows the power to EM mapping (Z) which is the ratio of the V_{probe} and I_{sup}. We can clearly see that the transfer function remains independent of the number of switching events at the operating frequency of 1GHz. This is as expected, since the amount of current drawn from the supply (I_{sup}) and the voltage induced across the EM probe (V_{probe}) should remain linear at low frequencies. This is an important result and the key take-away is that **the power to EM mapping for a given circuit is now possible by only shorting a few transistors instead of all, making it easier to scale across larger circuits**.

Now, as seen in Fig. 10, the transfer function (Z) remains constant (curves overlap) for all the different transistor switching patterns, and the mapping remains linear across different frequencies up to 10GHz. Most of today's embedded devices operate below this frequency limit, and frequency scaling in a core is limited due to the energy constraints and the thermal density, leading towards multi-core architectures since the last

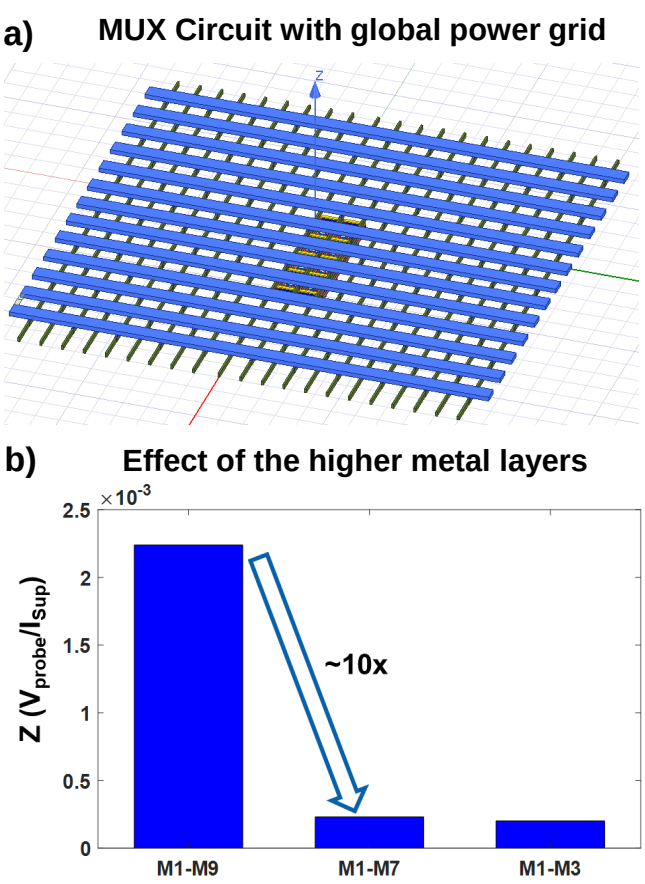

Fig. 11: Effect of the higher metal layers is demonstrated. (a) The MUX circuit is designed with the global power grid, emulating the global supply and ground for the entire IC (instead of just the local circuit under analysis). (b) These top metal layers (M8, M9 for the TSMC 65nm technology), which forms the global power grid contribute significantly to the EM leakage compared to the lower metal layers, re-validating the prior works [5], [9].

couple of decades. Hence, the important take-away from this result is that the power to EM mapping (Z) scales linearly with frequency, which is consistent with Biot Savart's Law, proving the magneto-quasistatic (MQS) approximation at the low frequency range. Note that, the metal layers have resonant peaks at the THz frequency range, but we are only concerned below 10GHz, where the transfer function remains linear with frequency. This is the main reason why the power to EM mapping is performed in the frequency domain as it would alleviate the need for measuring the transfer function Z across all the frequencies (utilizing the linear mapping).

D. Scalability to real crypto implementations: Elimination of the lower metal layers

Till now, in this section we have analyzed the 16:8 MUX circuit with only ~ 50 transistors. However, real-world crypto primitives like the S-Box or a full AES would have $1000\times$ more transistors. Modeling the full circuit in HFSS is complicated as it cannot be handled by the graphics support. As

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCAD.2022.3144369, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems

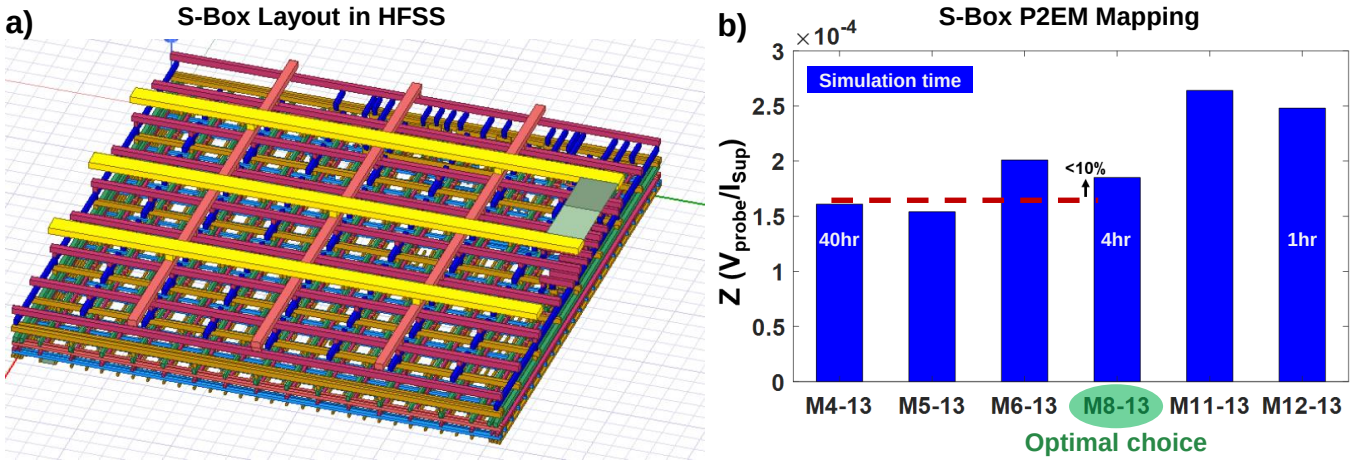

Fig. 12: S-Box power to EM mapping: (a) S-Box layout and its 3D modeling in HFSS; (b) the power to EM mapping for S-Box circuit.

of early 2021, even a powerful machine with 16 cores, 100 GB RAM was unable to load the S-Box circuit fully, due to graphics limitations (most likely owing to the millions of small dimension metals in the lower layers).

Now, it is known from prior works [9] that the higher metal layers of an integrated circuit contributes the most to the EM leakage, due to its higher thickness and longer length of routing (global power grid). Hence, as seen in Fig. 11(a, b), modeling the MUX circuit with the global power grid on the top two metal layers, the effect of the higher-level metal layers is re-validated (with previous work [9]) since removing just the top two metals reduces the EM leakage drastically by $\sim 10\times$. Now, with this understanding that the higher metal layers are the main contributors of the EM leakage, we can remove some of the bottom metal layers and obtain the power to EM mapping (Z). This would help scale to larger circuits like the S-Box or even an AES.

E. Results: S-Box CEMA

For scaling towards larger circuits, we consider a S-box implementation, which is a security primitive for symmetric key algorithms like AES. This application-based study has been performed in the Intel 10nm process (Fig. 12), which has 13 metal layers (M1-M13) [34]. The layout of the S-Box is generated using the commercial automatic place and route (APR) tools. As discussed earlier, the higher metal layers contribute significantly more to the EM SCA leakage compared to the lower metal layers, and hence we model the S-box layout in HFSS (Fig. 12(a)), starting from metal layer 4 (M4) and then removing one layer at a time to determine the optimum point for the power to EM mapping (Z) for this particular technology. As seen from Fig. 12(b), as we remove one layer at a time, the simulation time reduces drastically, while the accuracy of the power to EM mapping (Z) also reduces. Analyzing the layout structure, we observe that the power to EM mapping starting from metal layer M8 going up to metal M13 is the most optimal choice in terms of the simulation time and accuracy for this particular technology (Intel 10nm).

As discussed earlier, it is not feasible to simulate a large circuit with the entire metal stack due to its sheer complexity with all the transistors (and numerous tiny metal-via structures) at the lowest layer. Hence, the optimal choice of simulation from M8-M13 (for the Intel 10nm process) simplifies the flow and allows us to form an estimate of the EM SCA leakage in pre-Si environment, which is critical to evaluate the efficacy of a crypto engine and its countermeasure, prior to fabrication.

Note that, the power to EM mapping is only required to be computed at one frequency of interest (1 GHz, for our case), as it can be linearly scaled across other frequencies (Fig. 10), as evidenced by the MQS region of operation at these low frequencies and the geometry of the radiating elements, that is, the IC metal layer dimensions. Now, once the power to EM mapping (Z) is obtained from our HFSS model, we simultaneously simulate the S-box circuit using Virtuoso to obtain the power traces in the time-domain. The power traces are transformed to the frequency domain using FFT (Fig. 13(a), red curve), and the power to EM transfer function (Z) is applied on the power traces to obtain the corresponding EM traces in the frequency domain (Fig. 13(b), blue curve). Now, we perform a correlational power analysis (CPA) on the frequency-domain power traces using the hamming weight model as shown in Fig. 13(b) which reveals the correct key in $\sim$ 10 traces. CEMA is performed on the transformed frequency-domain EM traces which also successfully reveals the correct key in ~ 50 traces, validating the proposed HFSS-based framework. Similarly, the CEMA can also be performed in the time domain after transforming the generated frequency domain EM traces to the time domain through inverse FFT (IFFT), as discussed earlier (Sec. V.C, Fig. 8). The minimum traces to disclosure (MTD) is low since the noise is not added to the system, which can be modeled independently based on the system under consideration.

F. Discussion & Remarks

For the pre-Si EM SCA evaluation tool flow, the framework utilizes both Cadence Virtuoso and Ansys HFSS which are

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCAD.2022.3144369, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems

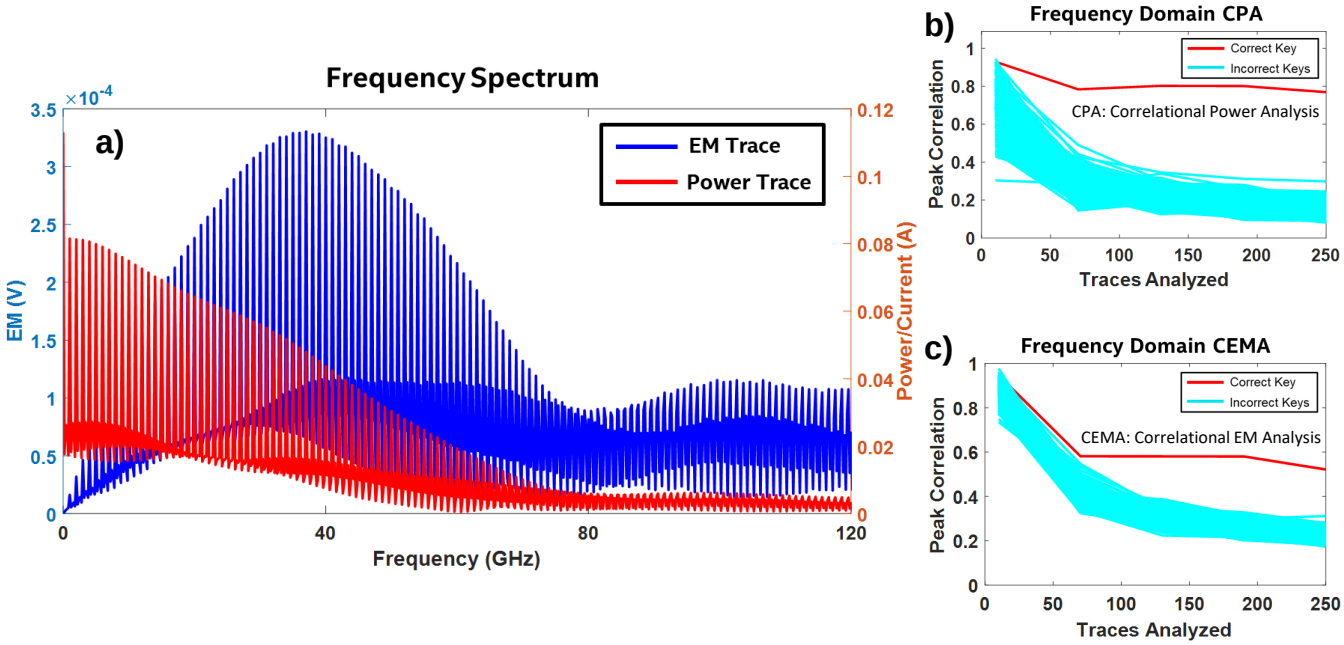

Fig. 13: S-Box CEMA: (a) Frequency spectrum of the power traces (red curve) and the transformed EM traces (blue curve) using our proposed framework. (b) Frequency-domain CPA shows the correct key separating out in $\sim$ 10 traces, while (c) CEMA attack shows the correct key extracted in $\sim$ 50 traces, validating the proposed pre-Si EM side-channel evaluation framework.

used commercially across the industry. Hence, all the file formats used are standard and are widely adopted. First, once the layout of the block is finalized, it is then exported as a GDS-II format file from Virtuoso and is imported in HFSS using a technology file (.tech extension) that maps the different layers of the GDS-II file to form the 3D metal-interconnect stack. Note that, both the GDS-II and the technology files are specific to a particular technology.

The main time-consuming step in the proposed HFSS-based pre-Si EM SCA evaluation framework is the loading of the circuit design in HFSS from Cadence Virtuoso (gds2 file) and mapping it to the exact dimensions of the metal-interconnect stack for the particular technology under consideration (using the .tech file). Even with a very powerful Intel CPU with 128 GB RAM, loading the AES128 consumes more than an hour due to the graphics limitations with the nanometer-scale objects. Hence, we believe that if the HFSS modeling can be performed through the command line instead of the GUI, it will alleviate the long loading time, thereby making it easier to scale to even larger circuits. This is however a future direction of work and needs to be performed in collaboration with the industry.

Overall, we propose the following steps to completely minimize both the local as well as the global EM leakage:

1) Use the double-row power grid layout technique to minimize the gate-level leakage.
2) Utilize the previously proposed technique in the form of STELLAR [9] for reducing the global leakage. STELLAR encapsulates the secure logic routed within the lower-level metal layers and then significantly suppresses the critical correlated current signature before it reaches the higher metal layers. Note that STELLAR alone does not suppress the local metal layer leakage. A combination of (1) and (2) guarantees maximal EM SCA security.
3) Now, instead of STELLAR, we can also utilize multi-pole routing in the higher metal layers for global EM leakage cancellation as described in [8].
4) To simulate the effect of (1) and (2) utilizing the pre-Si EM SCA security evaluation framework, we can independently evaluate the EM leakage from: (a) the local circuit encapsulated by STELLAR to obtain the effect of (1), and (b) the higher metal layers to get a sense of the attenuated current signature's EM leakage reduction.

VI. Conclusion & Future Work

To summarize, this work developed a framework to perform white-box modeling of the EM leakage from a crypto IC and proposed a new digital gate layout architecture to minimize the EM leakage. Using the HFSS-based framework, it was demonstrated that the double-row power grid layout pattern (supply-ground-supply (SGS)) for digital logic gates has significantly lower leakage compared to the traditional single-row layout pattern (supply-ground (SG)). This is a generic technique, which is agnostic of any crypto algorithms and has minimal area and power overheads and does not incur any performance overhead. For practical large design layouts, we proposed using the traditional standard library cells for the unrelated digital logic gates (other than crypto), while the

proposed double-row-based modified digital gate layouts for the security-critical logic to minimize the SNR significantly and thereby prevent EM SCA attacks.

The HFSS-based framework is extended to develop a pre-Si EM SCA evaluation technique combining both Virtuoso and HFSS. Hence, CEMA can now be performed during the design phase itself, which is extremely useful to evaluate the crypto implementations and countermeasures before a chip is fabricated, thereby reducing the time to market drastically for security sensitive designs.

REFERENCES

[1] Paul Kocher, Joshua Jaffe, and Benjamin Jun. Differential Power Analysis. In Michael Wiener, editor, *Advances in Cryptology — CRYPTO' 99*, Lecture Notes in Computer Science, pages 388–397. Springer Berlin Heidelberg, 1999.

[2] Karine Gandolfi, Christophe Mourtel, and Francis Olivier. Electromagnetic Analysis: Concrete Results. In *Cryptographic Hardware and Embedded Systems — CHES 2001*, Lecture Notes in Computer Science, pages 251–261. Springer, Berlin, Heidelberg, May 2001.

[3] Dakshi Agrawal, Bruce Archambeault, Josyula R. Rao, and Pankaj Rohatgi. The EM Side—Channel(s). In *Cryptographic Hardware and Embedded Systems - CHES 2002*, Lecture Notes in Computer Science, pages 29–45. Springer, Berlin, Heidelberg, August 2002.

[4] Craig Ramsay and Jasper Lohuis. TEMPEST attacks against AES. Technical report, Fox IT, 2017.

[5] D. Das, J. Danial, A. Golder, N. Modak, S. Maity, B. Chatterjee, D.-H. Seo, M. Chang, A. L. Varna, H. K. Krishnamurthy, S. Mathew, S. Ghosh, A. Raychowdhury, and S. Sen. EM and Power SCA-Resilient AES-256 Through >350x Current-Domain Signature Attenuation and Local Lower Metal Routing. *IEEE Journal of Solid-State Circuits*, pages 1–1, 2020. Conference Name: IEEE Journal of Solid-State Circuits.

[6] Debayan Das and Shreyas Sen. Electromagnetic and Power Side-Channel Analysis: Advanced Attacks and Low-Overhead Generic Countermeasures through White-Box Approach. *Cryptography*, 4(4):30, December 2020. Number: 4 Publisher: Multidisciplinary Digital Publishing Institute.

[7] Davide Poggi, Thomas Ordas, Alexandre Sarafianos, and Philippe Maurine. Checking Robustness Against EM Side-Channel Attacks Prior to Manufacturing. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, pages 1–1, 2021. Conference Name: IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems.

[8] Mayukh Nath, Debayan Das, and Shreyas Sen. A Multipole Approach Toward On-Chip Metal Routing for Reduced EM Side-Channel Leakage. *IEEE Microwave and Wireless Components Letters*, 31(6):685–688, June 2021. Conference Name: IEEE Microwave and Wireless Components Letters.

[9] D. Das, M. Nath, B. Chatterjee, Santosh Ghosh, and Shreyas Sen. STELLAR: A Generic EM Side-Channel Attack Protection through Ground-Up Root-cause Analysis. In *2019 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pages 11–20, May 2019.

[10] Debayan Das, Josef Danial, Anupam Golder, Nirmoy Modak, Shovan Maity, Baibhab Chatterjee, Donghyun Seo, Muya Chang, Avinash Varna, Harish Krishnamurthy, Sanu Mathew, Santosh Ghosh, Arijit Raychowdhury, and Shreyas Sen. 27.3 EM and Power SCA-Resilient AES-256 in 65nm CMOS Through >350× Current-Domain Signature Attenuation. In *2020 IEEE International Solid- State Circuits Conference - (ISSCC)*, pages 424–426, February 2020. ISSN: 2376-8606.

[11] Amit Kumar, Cody Scarborough, Ali Yilmaz, and Michael Orshansky. Efficient simulation of EM side-channel attack resilience. In *2017 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, pages 123–130, November 2017. ISSN: 1558-2434.

[12] Victor Lomné, Philippe Maurine, Lionel Torres, Thomas Ordas, Mathieu Lisart, and Jérome Toublanc. Modeling Time Domain Magnetic Emissions of ICs. In René van Leuken and Gilles Sicard, editors, *Integrated Circuit and System Design. Power and Timing Modeling, Optimization, and Simulation*, Lecture Notes in Computer Science, pages 238–249, Berlin, Heidelberg, 2011. Springer.

[13] Eyal Ronen, Adi Shamir, Achi-Or Weingarten, and Colin O'Flynn. IoT Goes Nuclear: Creating a ZigBee Chain Reaction. In *2017 IEEE Symposium on Security and Privacy (SP)*, pages 195–212, May 2017. ISSN: 2375-1207.

[14] Daniel Genkin, Lev Pachmanov, Itamar Pipman, and Eran Tromer. ECDH Key-Extraction via Low-Bandwidth Electromagnetic Attacks on PCs. Technical Report 129, 2016.

[15] Giovanni Camurati, Sebastian Poeplau, Marius Muench, Tom Hayes, and Aurélien Francillon. Screaming Channels: When Electromagnetic Side Channels Meet Radio Transceivers. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, CCS '18, pages 163–177, Toronto, Canada, January 2018. Association for Computing Machinery.

[16] Josef Danial, Debayan Das, Santosh Ghosh, Arijit Raychowdhury, and Shreyas Sen. SCNIFFER: Low-Cost, Automated, Efficient Electromagnetic Side-Channel Sniffing. *IEEE Access*, 8:173414–173427, 2020. Conference Name: IEEE Access.

[17] Oleksiy Lisovets, David Knichel, Thorben Moos, and Amir Moradi. Let's Take it Offline: Boosting Brute-Force Attacks on iPhone's User Authentication through SCA. Technical Report 460, 2021.

[18] Victor LOMNE and Thomas ROCHE. A Side Journey to Titan. Technical Report 028, 2021.

[19] Debayan Das, Anupam Golder, Josef Danial, Santosh Ghosh, Arijit Raychowdhury, and Shreyas Sen. X-DeepSCA: Cross-Device Deep Learning Side Channel Attack. In *2019 56th ACM/IEEE Design Automation Conference (DAC)*, pages 1–6, June 2019. ISSN: 0738-100X.

[20] Houssem Maghrebi, Thibault Portigliatti, and Emmanuel Prouff. Breaking Cryptographic Implementations Using Deep Learning Techniques. Technical Report 921, 2016.

[21] Anupam Golder, Debayan Das, Josef Danial, Santosh Ghosh, Shreyas Sen, and Arijit Raychowdhury. Practical Approaches Toward Deep-Learning-Based Cross-Device Power Side-Channel Attack. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 27(12):2720–2733, December 2019.

[22] Sikhar Patranabis, Debapriya Basu Roy, Anirban Chakraborty, Naveen Nagar, Astikey Singh, Debdeep Mukhopadhyay, and Santosh Ghosh. Lightweight Design-for-Security Strategies for Combined Countermeasures Against Side Channel and Fault Analysis in IoT Applications. *Journal of Hardware and Systems Security*, 3(2):103–131, June 2019.

[23] M. Arsath K. F, V. Ganesan, R. Bodduna, and C. Rebeiro. PARAM: A Microprocessor Hardened for Power Side-Channel Attack Resistance. In *2020 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pages 23–34, December 2020.

[24] Oscar Reparaz, Begül Bilgin, Svetla Nikova, Benedikt Gierlichs, and Ingrid Verbauwhede. Consolidating Masking Schemes. In Rosario Gennaro and Matthew Robshaw, editors, *Advances in Cryptology – CRYPTO 2015*, Lecture Notes in Computer Science, pages 764–783. Springer Berlin Heidelberg, 2015.

[25] Arvind Singh, Monodeep Kar, Venkata Chaitanya Krishna Chekuri, Sanu K. Mathew, Anand Rajan, Vivek De, and Saibal Mukhopadhyay. Enhanced Power and Electromagnetic SCA Resistance of Encryption Engines via a Security-Aware Integrated All-Digital LDO. *IEEE Journal of Solid-State Circuits*, 55(2):478–493, February 2020.

[26] W. Yu and S. Köse. Exploiting Voltage Regulators to Enhance Various Power Attack Countermeasures. *IEEE Transactions on Emerging Topics in Computing*, 6(2):244–257, April 2018. Conference Name: IEEE Transactions on Emerging Topics in Computing.

[27] C. Tokunaga and D. Blaauw. Securing Encryption Systems With a Switched Capacitor Current Equalizer. *IEEE Journal of Solid-State Circuits*, 45(1):23–31, January 2010.

[28] 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 *2017 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pages 62–67, May 2017.

[29] Debayan Das, Shovan Maity, Saad Bin Nasir, Santosh Ghosh, Arijit Raychowdhury, and Shreyas Sen. ASNI: Attenuated Signature Noise Injection for Low-Overhead Power Side-Channel Attack Immunity. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 65(10):3300–3311, October 2018.

[30] Patanjali Slpsk, Prasanna Karthik Vairam, Chester Rebeiro, and V. Kamakoti. Karna: A Gate-Sizing based Security Aware EDA Flow for Improved Power Side-Channel Attack Protection. In *2019 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, pages 1–8, November 2019. ISSN: 1558-2434.

[31] Yuan Yao, Tarun Kathuria, Baris Ege, and Patrick Schaumont. Architecture Correlation Analysis (ACA): Identifying the Source of Side-channel Leakage at Gate-level. In *2020 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pages 188–196, December 2020.

[32] D. D. Hwang, K. Tiri, A. Hodjat, B. C. Lai, S. Yang, P. Schaumont, and I. Verbauwhede. AES-Based Security Coprocessor IC in 0.18um CMOS With Resistance to Differential Power Analysis Side-Channel Attacks. *IEEE Journal of Solid-State Circuits*, 41(4):781–792, April 2006.

[33] Bruce Jacob, Spencer W. Ng, and David T. Wang. CHAPTER 8 - DRAM Device Organization: Basic Circuits and Architecture. In Bruce Jacob, Spencer W. Ng, and David T. Wang, editors, *Memory Systems*, pages 353–376. Morgan Kaufmann, San Francisco, January 2008.

[34] C. Auth, A. Aliyarukunju, M. Asoro, D. Bergstrom, V. Bhagwat, J. Birdsall, N. Bisnik, M. Buehler, V. Chikarmane, G. Ding, Q. Fu, H. Gomez, W. Han, D. Hanken, M. Haran, M. Hattendorf, R. Heussner, H. Hiramatsu, B. Ho, S. Jaloviar, I. Jin, S. Joshi, S. Kirby, S. Kosaraju, H. Kothari, G. Leatherman, K. Lee, J. Leib, A. Madhavan, K. Marla, H. Meyer, T. Mule, C. Parker, S. Parthasarathy, C. Pelto, L. Pipes, I. Post, M. Prince, A. Rahman, S. Rajamani, A. Saha, J. Dacuna Santos, M. Sharma, V. Sharma, J. Shin, P. Sinha, P. Smith, M. Sprinkle, A. St. Amour, C. Staus, R. Suri, D. Towner, A. Tripathi, A. Tura, C. Ward, and A. Yeoh. A 10nm high performance and low-power CMOS technology featuring 3rd generation FinFET transistors, Self-Aligned Quad Patterning, contact over active gate and cobalt local interconnects. In *2017 IEEE International Electron Devices Meeting (IEDM)*, pages 29.1.1–29.1.4, December 2017. ISSN: 2156-017X.

Debayan Das (S'17, M'21) completed his PhD in Electrical and Computer Engineering at Purdue University in 2021 and is currently working as a Security Researcher with Intel Corporation. He received his Bachelor of Electronics and Telecommunication Engineering from Jadavpur University, India, in 2015. Prior to joining PhD, he worked as an Analog Design Engineer at a start-up based in India. He has interned with the Security Research Lab, Intel Labs, OR, over the summers of 2018 and 2020. His research interests include hardware security and mixed-signal IC design.

Debayan was a recipient of the IEEE HOST Best Student Paper Award in 2017, 2019, CICC 2021 Best Student Paper Award, the 2nd Best Demo Award in HOST 2020, and the 3rd Best Poster Award in IEEE HOST 2018. In 2019, one of his papers was recognized as a Top Pick in Hardware & Embedded Security published over the span of last six years. He was recognized as the winner (third place) of the ACM ICCAD 2020 Student Research Competition (SRC). During his Ph.D., he has been awarded the ECE Fellowship during 2016–2018, the SSCS Pre-doctoral Achievement Award in 2020-21, the Bilsland Dissertation Fellowship (2020–2021), and the Outstanding Graduate Student Research Award by the College of Engineering, Purdue University.

Mayukh Nath (S'20) received the B.S. degree in physics from the Indian Institute of Science, Bengaluru, India, in 2016. He is currently pursuing the Ph.D. degree in electrical engineering with Purdue University, West Lafayette, IN, USA. His research interests include electromagnetic theory and simulation-based formulation of inter-device communications, such as body area network-based medical implants and wearables. He is also interested in electromagnetism based fundamental formulation of side channel attack and prevention techniques.

Baibhab Chatterjee (S'17, M'22) received the B.Tech. degree in electronics and communication engineering from the National Institute of Technology (NIT), Durgapur, India, in 2011, and the M.Tech. degree in electrical engineering from IIT Bombay, Mumbai, India, in 2015. He is currently pursuing the Ph.D. degree with the School of Electrical Engineering, Purdue University, West Lafayette, IN, USA. His industry experience includes two years as a Digital Design Engineer/a Senior Digital Design Engineer with Intel, Bengaluru, India, and one year as a Research and Development Engineer with Tejas Networks, Bengaluru. His research interests include low-power analog, RF, and mixed-signal circuit design for secure biomedical applications.

Mr. Chatterjee received the University Gold Medal from NIT, Durgapur, India, in 2011, the Institute Silver Medal from IIT Bombay in 2015, the Andrews Fellowship at Purdue University during 2017-2019, the HOST 2018 Best Student Poster Award (3rd), the CICC 2019 Best Paper Award (overall), the RFIC/IMS 2020 3MT Award (audience choice) and the Bilsland Fellowship at Purdue University during 2021-2022.

Raghavan Kumar (M'13-SM'21) received the M.S., and Ph.D. degrees in Electrical Engineering from the University of Massachusetts in 2012 and 2015, respectively. He is currently a staff research scientist with Circuit Research Labs, Intel Hillsboro, OR. His research interests include hardware security, machine learning, homomorphic encryption, and high performance and low power datapath circuits. He has authored over 35 technical articles, 2 book chapters and holds 15 U.S issued patents with more than 50 patents pending.

Xiaosen Liu (S'08–M'16) received the B.S. degree in electrical engineering from the Southeast University, Nanjing, China, the M.Phil. degree from the Hong Kong University of Science and Technology, Hong Kong, and the Ph.D. degree from the Texas A&M University, College Station, in 2008, 2011, and 2016. He is currently a Research Scientist in Circuit Research Lab of Intel Labs, OR, USA.

He was a recipient of the 2015-2016 Solid-State Circuits Society Predoctoral Achievement Award, 2016 Chinese Government Award For Outstanding Self-Financed Students Abroad, the TPC member IEEE DAC, SOCC, MWSCAS, ISQED. His current research interests include power management for next-generation SoC, energy harvesting, wide-bandgap electronics, and electrosurgical instruments.

Harish K Krishnamurthy is a Principal Engineer in the Circuits Research Lab in Intel Labs working on power delivery circuits and systems. He graduated from Arizona State University with a PhD degree in Electrical Engineering in 2008. His research interests include topologies and digital control techniques for fully on-die switching power converters, fully synthesizable digital LDOs and reconfigurable power delivery. He has over 25 publications at leading IEEE conferences, over 20 issued patents, and over 30 patent applications filed to date, and is currently serving as a Technical Program Committee member for the Power management sub-committee at ISSCC (International Solid-State Circuits Conference).

Manoj Sastry is a Principal Engineer in Intel Labs. He is responsible for driving research in the area of cryptography and cybersecurity for autonomous systems. He has more than 25 years of industry experience related to cybersecurity, trusted platforms, system-on-chip, networks, IoT, side-channels, and lightweight & post-quantum cryptography. He has published 27 papers and filed 125 patents.

Sanu 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. He is currently a Senior Principal Engineer with Circuits Research Lab, Intel Corporation, Hillsboro, OR, USA, where he heads the Security Arithmetic Circuits Research Group, responsible for developing energy-efficient computer arithmetic data-path circuits and special-purpose hardware accelerators for cryptography and security. He has been with Intel Corporation since 1999. He has received two Intel Achievement Awards for pioneering energy-efficient execution core integer datapaths circuit technologies and developing AES-NI hardware on Intel products. He holds 110 issued/pending patents, has published 86 conference/journal articles and authored two book chapters. Dr. Mathew also mentors Intel- and Semiconductor Research Corporation (SRC)-funded research projects in leading universities and has served on the program committees of the International Symposium on Computer Arithmetic (ARITH), the International Symposium on Low Power Electronics and Design (ISLPED), Design Automation Conference (DAC), and the International System-on-Chip Conference (SOCC) conferences. He currently serves on the technical program committee at International Solid-State Circuits Committee (ISSCC).

Santosh Ghosh is a Research Scientist in Intel Labs. He has coauthored about 69 research publications in refereed international conferences and journals with a citation H-index of 21, and 22 issued with other 55 more patents filed (pending). The primary focus of his research includes: 1) Lightweight and post-quantum crypto algorithms; 2) low overhead innovative processor micro-architecture using lightweight crypto to solve long-lasting SW bugs & vulnerabilities and to protect side-channel attacks; 3) cryptographic hardware microarchitecture and RTL with the aggressive area, latency, and throughput constraints; multiple of them are already being deployed in high-volume Intel products; and 4) investigate and develop timing, power, EM and Photon side-channel countermeasures. Santosh received the Ph.D. degree from IIT Kharagpur, India in 2011, and completed his post-doctoral studies from COSIC, KU Leuven, Leuven, Belgium, in the area of cryptographic hardware and side-channel attacks.

Shreyas Sen (S'06-M'11-SM'17) is an Associate Professor in ECE, Purdue University and received his Ph.D. degree in ECE, Georgia Tech. Dr. Sen has over 5 years of industry research experience in Intel Labs, Qualcomm and Rambus. His current research interests span mixed-signal circuits/systems and electromagnetics for the Internet of Things (IoT), Biomedical, and Security. Dr. Sen is the inventor of the Electro-Quasistatic Human Body Communication, for which, he is the recipient of the MIT Technology Review top-10 Indian Inventor Worldwide under 35 (MIT TR35 India) Award. Dr. Sen's work has been covered by 100+ news releases worldwide, invited appearance on TEDx Indianapolis, Indian National Television CNBC TV18 Young Turks Program and NPR subsidiary Lakeshore Public Radio. Dr. Sen is a recipient of the NSF CAREER Award 2020, AFOSR Young Investigator Award 2016, NSF CISE CRII Award 2017, Google Faculty Research Award 2017, Intel Labs Quality Award for industrywide impact on USB-C type, Intel Ph.D. Fellowship 2010, IEEE Microwave Fellowship 2008 and seven best paper awards including IEEE CICC 2019 and IEEE HOST 2017, 2018, and 2019. Dr. Sen's work was chosen as one of the top-10 papers in the Hardware Security field over the past 6 years (TopPicks 2019). He has co-authored 2 book chapters, over 135 journal and conference papers, and has 14 patents granted/pending. He serves/has served as an Associate Editor for IEEE Design & Test, Executive Committee member of IEEE Central Indiana Section and Technical Program Committee member of DAC, CICC, DATE, ISLPED, ICCAD, ITC, VLSI Design, among others. Dr. Sen is a Senior Member of IEEE.