EMSIM: A Fast Layout Level Electromagnetic Emanation Simulation Framework for High Accuracy Pre-Silicon Verification

Haocheng Ma, Max Panoff, *Graduate Student Member, IEEE*, Jiaji He, Yiqiang Zhao, *Member, IEEE*, and Yier Jin, *Senior Member, IEEE*

***Abstract*— Electromagnetic (EM) emanation measurement and evaluation is one important testing for modern integrated circuits (ICs). Severe electromagnetic interference may degrade the performance of electronic devices or even cause system crashes. As a result, modern ICs need to follow strict electromagnetic compatibility (EMC) requirements. Moreover, EM emanations offer a covert channel for adversaries to steal secret information from fabricated ICs, causing side channel attacks. Due to the lack of fast and high-accuracy EM simulation tools, existing EM measurements often happen at the post-silicon stage. Any identification of side channel vulnerability or EM incompatibility may lead to high cost and delay the time-to-market. As a result, design-time EM simulation tools with fast simulation speed and high accuracy for pre-silicon designs are urgently needed. To this end, we propose EMSIM, a layout-level EM simulation framework that significantly speeds up the EM simulation process while maintaining high accuracy of the simulated EM emanations. To achieve this goal, we provide the theoretical explanation for the root cause of EM emanations from ICs. Guiding by this, EMSIM leverages techniques of parasitic network reduction and device model approximation to reduce the computation complexities while still ensuring high simulation accuracy. EMSIM further leverages Graphics Processing Unit (GPU) resources to solve equations for EM simulation. The efficiency and effectiveness of EMSIM are validated by showing the consistency between simulation results and physical measurements obtained from fabricated circuit designs.**

***Index Terms*— CAD for security, EM emanation simulation, side channel analysis.**

I. INTRODUCTION

INTEGRATED circuits development has become increasingly challenging due to the high-dense on-chip transistor counts. As a result, electronic design automation (EDA) tools are of great importance for designers to guarantee a successful tape-out. The involvement of simulation-driven algorithms facilitates tackling the challenges during IC development such as power budgeting, signal integrity, thermal stress and electrostatic discharge (ESD) reliability. However, designers rarely consider the challenge raised by EM emanations, which potentially jeopardize the functional safety and information security of electronic systems. Note that ICs are often the ultimate source of unintentional electromagnetic (EM) emissions from electronic systems. EM emanations stem from current flow inside IC components, create electromagnetic interference issues through conducted emission and radiation emission [1]. Further, EM emanations contain rich information in spatial, temporal and frequency domains and can be collected and measured without direct physical contact. This makes hardware implementations like cryptographic or neural network algorithms vulnerable to EM side-channel analysis (SCA) [2], [3]. EM SCA attack is the process of analyzing EM emanations through which attackers can extract sensitive internal information. In view of the above risks, it is critical to take the EM simulation into account before delivering the physical design to the foundry. This is especially true for ICs deployed in critical applications include autonomous vehicles, electronic banking, mobile communication, and cloud computing and storage [4]. The inevitable challenge here is the absence of well-established commercial EDA tools with respect to simulating EM emanation from pre-fabrication designs. Most of the existing tools, like Ansys HFSS [5], are designed for simulating electronic products such as antennas, filters, connectors, IC packages and printed circuit boards (PCB). They are not adapted for simulating ICs comprised of complex power supply, electrical interconnection and multifunctional logic cells.

When ICs operate, logic cells create varying currents across metal layers due to switching activities. Metal wires carrying time-varying currents act as antennas and emit EM emanations. Therefore, the prediction of EM emanations can be achieved in two steps. First, multi-level circuit analysis is carried out to obtain the current profiles distributed on the physical layout. Then based on the EM field principle, the probed EM emanations are calculated from the current profiles. According to the ICs design phases, data at the register-transfer level (RTL) and gate-level can only support the estimation of the current profiles. While layout-level data contains all the

Manuscript received 22 August 2021; revised 27 December 2021 and 9 March 2022; accepted 2 January 2023. Date of publication 23 January 2023; date of current version 2 February 2023. This work was supported in part by the National Key Research and Development Program of China under Grant 2021YFB3100903 and in part by the National Natural Science Foundation of China under Grant 62004112. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Valeria Loscri. *(Corresponding authors: Jiaji He; Yiqiang Zhao.)*

Haocheng Ma, Jiaji He, and Yiqiang Zhao are with the School of Microelectronics, Tianjin University, Tianjin 300072, China (e-mail: hc_ma@tju.edu.cn; dochejj@tju.edu.cn; yq_zhao@tju.edu.cn).

Max Panoff and Yier Jin are with the Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL 32611 USA (e-mail: m.panoff@ufl.edu; yier.jin@ece.ufl.edu).

Digital Object Identifier 10.1109/TIFS.2023.3239184

physical information of the fabricated ICs, with which the simulation results can more accurately indicate the spatial, temporal and amplitude characteristics of EM emanations [6], [7], [8], [9]. However, as circuit sizes grows quickly, so are the sizes of extracted parasitic networks. The complexity of simulated device models grows exponentially, leading to slower simulations especially for large circuits. Prior work has done much to alleviate this burden. For example, the authors in [8] restrict current simulation to wires that have a larger impact on the final EM field near a device. These existing methods still rely on high accuracy transistor-level simulation on the concerned time windows. Further, existing approaches are rarely verified by the physical measurements.

Upon these challenges, in this paper, we propose a novel fast EM simulation process, named **EMSIM: Electromagnetic emanation Simulation at early design phrase**, for digital circuits.[1] To achieve this goal, we first analyze the physical essence of IC's EM emanations and provide theoretical explanations for our simplification. The key idea of EMSIM is in the simplification of current analysis, i.e., using device model approximation and parasitic network reduction. Specifically, for device model approximation we propose a method to simulate logic cells as time-based current sources. Parasitic network reduction will further filter the non-critical parasitic information, e.g., interconnect wire, before Spice-level simulation. These techniques greatly reduce computational load while keeping current flows within wires close to their true values for accurate security evaluations. Furthermore, we model the magnetic field from multiple wires as multidimensional matrices. Supported by the NumPy library [10] and CuPy library [11], EMSIM provides two computation modes enabling the solution of these equations on either CPUs or GPUs. CuPy accelerates simulations for large-scale circuits by fully exploiting the computing power of GPUs.[2] These strategies help greatly decrease computational cost while still provide sufficiently accurate simulation results so that chip designers can better understand the EM emanation.

The main contributions of the paper are as follows.

- We build the explanation model to explore the root cause of EM emanations and the key elements which dominate in the EM generation and propagation. All of these constitute the theoretical foundation of our layout-level EM simulation.
- An EM simulation tool, named EMSIM, is developed to support EM security evaluation at the pre-silicon layout level. This tool can simulate and analyze the EM emanations automatically and is compatible with the existing EDA design flow.
- Various strategies are leveraged to speed up the simulation process of EMSIM such as the device model approximation and parasitic network reduction during current analysis, and GPU acceleration during EM computation. EMSIM offers high flexibility for the trade-off between the accuracy and the computation cost.
- We compare the simulation result accuracy of EMSIM with both the conventional EM simulation methods and silicon-level measurements obtained from fabricated circuits. The experimental results show that the developed EMSIM can provide high EM simulation accuracy with much fast simulation speed.

The rest of the paper is organized as follows. Section II goes over existing EM simulation process, security analysis and evaluation metrics. In Section III, the underlying cause of EM emanations from ICs are provided through an explanation model. Section IV introduces the overall framework of EMSIM. In Section V we present the results of EMSIM and compare the results with existing EM simulation methods. In Section VI and Section VII, we further compare EMSIM to experimental results measured from fabricated chips. Finally, we conclude the paper in Section IX.

II. BACKGROUND

A. EM Simulation Methodology

EM simulation aims to predict the EM behavior of electronic devices at the design stage. The conventional approach is to construct a three-dimensional (3-D) model using commercial EM simulators such as Ansys HFSS. EM emanations are obtained by solving Maxwell's equations using the 3-D model. This process can be extremely slow for EM simulation of ICs, due to a large number of metal wires and standard cells [12]. An alternative method is to build the behavioral model or electrical model of ICs to simplify EM simulation. Behavioral model-based approaches use design data like RTL code [13] or gate-level netlist [14] to mimic EM emanations. However, this type of methods do not consider the physical characteristics of the chip and produce low-accuracy results. The physical layout is utilized in the electrical model-based approach, which contains physical information of the fabricated ICs. Hence the simulation results obtained by the electrical model-based approach are closer to actual measurements of fabricated ICs.

As we mentioned earlier, the procedure of the electrical model-based approach falls into two steps. In Step 1, it carries out multi-level circuit analysis to obtain the current profiles distributed on the physical layout. In Step 2, based on the EM field principle, the probed EM emanations are calculated from the current profiles. To alleviate high computational complexities, various simplification methods have been applied to the above steps. In [7] and [15], only currents distributed across the top metal layers of the on-chip power distributed network (PDN) are used in Step 2. The authors in [8] propose hybrid-level circuit analysis to further accelerate the current profiles acquisition. These simplifications are based on the assumption that high amplitude currents often flow inside the top metal layers of the power grid, thus forming the main source of EM emanations. While experimental results are provided in [9], [12], and [16], there lacks theoretical analysis to support this assumption. In this paper, we provide a comprehensive explanation to investigate the underlying

[1] Source code of the EMSIM is released to the public and can be found at https://github.com/jinyier/EMSim

[2] Current EDA tools are mostly CPU-centric and one very few of them leverage the computation capability provided by new computing resources such as GPU and TPU.

cause of EM emanations. We further put forward a number of strategies to accelerate both steps.

B. EM Side Channel Analysis Attacks

Cryptographic algorithms are widely deployed in modern electronic systems and are often central to critical infrastructures for data security and privacy. Despite the fact that these algorithms are mathematically or computationally secure and are resistant to various algorithmic attacks [17], interactions between their hardware implementations and physical environment arise opportunities for SCA attacks. Examples of side channels include power consumption, timing delay, EM emanations, heat, optical leakage, etc. Similar to other SCA attacks, EM SCA attacks on cryptographic devices (or other devices) can be roughly divided into two stages. In the first stage, the EM emanations of the device performing encryption are collected. Near-field scanning systems are often used to take full advantage of the spatial characteristic. These measurements are taken across the chip's surface at specific test points and captured with high-resolution EM probes. Here we collect a set of traces $T_{n\times t\times p}$ where n, t, p denote the quantity of input stimulus, sampling points and probed positions, respectively.

In the second stage, the collected EM emanations are analyzed to recover the secret key (or other sensitive information). At this stage, various analysis methods will be applied including Simple Electromagnetic Analysis (SEMA), Differential Electromagnetic Analysis (DEMA), and Correlation Electromagnetic Analysis (CEMA) [18]. To resist EM analysis attacks, the defender has to iterate through security evaluation and countermeasure optimization at design time. During these security evaluations, the defender simulates the EM side-channel leakage and then applies assessment techniques like CEMA on the simulated traces. As shown in Equation (1), the Pearson correlation coefficient $\rho_{m\times t\times p}$ serves as a distinguisher in CEMA attacks. Hamming weight model [2] or Hamming distance model [13] is also exploited to build the predicted leakage matrix $W_{n\times m}$, where m is the amount of guessed secret key or other sensitive information.

$$\rho_{m\times t\times p} = \frac{\mu_{T_{n\times t\times p}\cdot W_{n\times m}} - \mu_{T_{n\times t\times p}}\cdot \mu_{W_{n\times m}}}{\sqrt{\sigma^2_{T_{n\times t\times p}}\cdot \sigma^2_{W_{n\times m}}}} \tag{1}$$

where μ and σ^2 are the average and variance of corresponding variables. The recovered key with the maximum Pearson correlation coefficient ρ_{max} indicates the most possible correct hypothesis. When the number of traces exceeds a certain value, the ρ_{max} of the correct hypothesis will always be greater than those of wrong guesses. This certain value, often named as measurement to disclosure (MtD), denotes the minimum traces to disclosure the key.

C. Simulation Evaluation Metric

For EM simulation, there is a demand to provide evidence that how well the simulated results match with the actual measurements. The classical proof depends on visual comparison to ensure that the credibility of simulation approaches [6], [7], [20], [21]. Since visual comparison is a subjective measure, we prefer a fair comparison where multiple aspects are assessed using quantitative metrics. These aspects include not only the EM emanation itself such as time, spatial and frequency characteristics but also their applications, such as side-channel security.

1) Metrics of Intrinsic Accuracy: There are many metrics to compare the similarity between two two-dimensional signals, including euclidean distance [22], coefficient of determination [23] and cross correlation. Similar to the work in [19], the normalized cross correlation is exploited in this paper, especially for comparing time-domain traces between EMSIM and other simulation approaches or actual measurements.

$$ncc = \frac{1}{N}\sum_{i=1}^{N}\frac{\sum_{t=1}^{T}(\|x\|_t^i - \|\bar{x}\|^i)(\|y\|_t^i - \|\bar{y}\|^i)}{\sqrt{\sum_{t=1}^{T}(\|x\|_t - \|\bar{x}\|^i)^2}\sqrt{\sum_{t=1}^{T}(\|y\|_t^i - \|\bar{y}\|^i)^2}} \tag{2}$$

As depicted in Equation (2), we first normalize both simulated signals x and actual signals y to the range $[-1, 1]$. The $\|x\|$ and $\|y\|$ denote the normalized data with T time points. Then we compute the cross correlation coefficient between normalized simulated data $\|x\|^i$ and actual data $\|y\|^i$ under each stimulus i. The final accuracy ncc is obtained by averaging these coefficients across all N stimuli. Similarly, the frequency characteristics are compared by metric ncc, while the frequency domain signals x and y are transformed by fast Fourier transform (FFT). Another important characteristic for EM emanations is the spatial distribution, embodied in the form of three-dimensional signals. Here we view these signals as images and search their differences using structural similarity index measure (SSIM) [24]. SSIM is used for measuring the similarity between two images, on the basis of their luminosity, contrast and structural difference. Let X and Y denote the three-dimensional matrices of simulated EM maps and real EM maps. The value $ssim$ can be computed as Equation (3).

$$ssim = \frac{(2\mu_X\mu_Y + C_1)(2\sigma_{XY} + C_2)}{(\mu_X^2 + \mu_Y^2 + C_1)(\sigma_X^2 + \sigma_Y^2 + C_1)} \tag{3}$$

where μ_X and μ_Y are the average of X and Y. σ_X, σ_Y are the standard deviation of X, Y, while σ_{XY} is the covariance of X and Y. C_1, C_2 and C_3 are constants to avoid the instability caused by the denominator being zero.

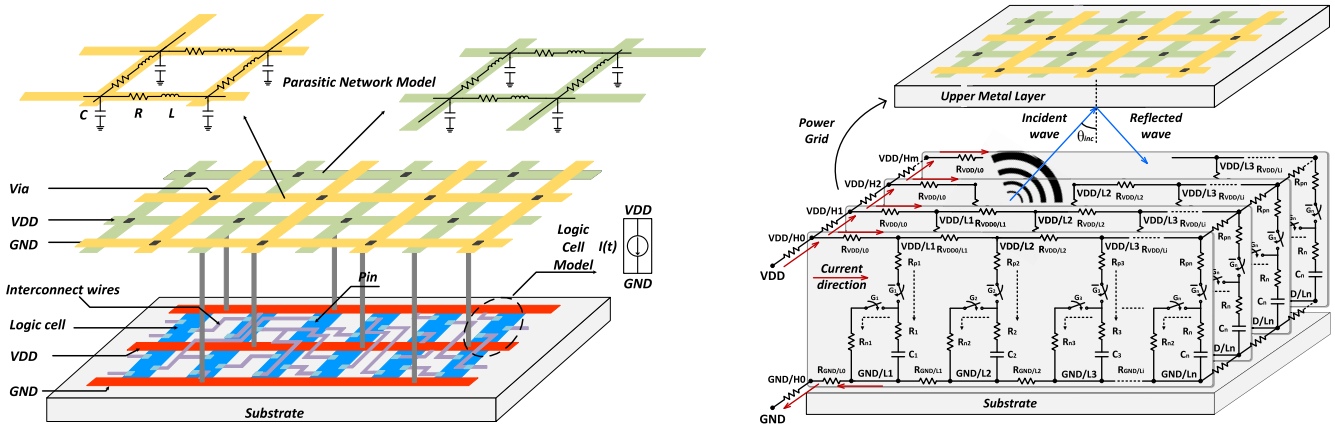
2) Metrics of Application Accuracy: In the context of simulation for side-channel security, there is also a demand for validating that the accuracy of simulations used for security evaluation. Typically, security evaluations are carried out by actual SCA attacks (e.g., CEMA) or leakage assessment techniques (e.g., test-vector leakage assessment (TVLA) [25]). However, TVLA suffers issues such as false positives. In some cases, the actual attack will not succeed although the TVLA predicts a positive leakage result [26]. Hence we prefer CEMA attacks during the security evaluation, leveraging the Pearson correlation coefficient and MtD as the security metrics.

A qualitative comparison between EMSIM and existing works is listed in Table I.

TABLE I
COMPARISON OF EMSIM WITH PRIOR WORKS

Method	Input Phase	Target Device	Efficacy			
			Time	Frequency	Spatial	Security Evaluation
ASP-DAC'2020 [13]	RTL	FPGA	-	-	-	✔
Integration'2007 [14]	Gate	ASIC	✔	-	-	-
PATMOS'2010 [7]	Layout	ASIC	✔	-	✔	-
ICCAD'2017 [8]	Layout	ASIC	-	-	-	-
TCAD'2021 [15]	Layout	ASIC	-	-	✔	✔
HPCA'2020 [19]	Post-Silicon	FPGA	✔	-	-	✔
This Work	Layout	ASIC	✔	✔	✔	✔

The symbol - denotes that no results are reported.



(a) physical topology (b) electrical model

Fig. 1. The physical topology and electrical model of an IC.

III. EMSIM: FUNDAMENTAL

Before we introduce EMSIM in detail, we will first provide an in-depth view of EM emanations from ICs and an understanding of which elements contribute with more proportion. Here we build an explanation model to clarify the above queries and constitute the fundamental of our proposed tool.

A. Model Construction

As shown in Figure 1 (a), digital Complementary metal–oxide–semiconductor (CMOS) based ICs can be characterized by two interdependent electrical systems, the logic cell network and parasitic network [27]. The logic cell network is formed by groups of transistors on the silicon substrate providing combinatorial and sequential logic functionality. A logic cell's pins include input/output pins and power-supply pins. The input and output pins transfer the logical signals in and out of the logic cells, under the support of interconnect wires. While power-supply pins provide the positive and negative supply voltage for logic cells, joined with the VDD and GND power grids. The power grid, when combined with interconnect wires, forms the parasitic network.

Metal wires carrying time-varying currents are the emitters of EM emanations. As a result, the parasitic network excited by the logic cell network is responsible for the circuit's EM emanations. Up to now, the widely accepted claim is that high amplitude currents flow within the top metal layers of the power grid, thus form the main source of EM emanations. This claim is experimentally verified in [9], [12], and [16] and adopted in most layout-level EM simulation approaches. However, there lacks theoretical analysis to support this claim. Within this context, we will first provide a comprehensive explanation of the underlying cause of EM emanations. The proposed explanation model illustrated in Figure 1 (b) is based on the electrical and structural characteristics of the IC. Take the positive power supply for instance. VDD denotes the power pins around the chip die boundary, and VDD/Hj, $j = 1, 2, \ldots m$ represent power nodes distributed in the top metal layers of the power grid. The subsequent power nodes in the lower metal layers of the power grid are denoted as VDD/Li, $i = 1, 2, \ldots n$. The supply power from external power pads will start with the VDD pins, pass through VDD/Hj and VDD/Li nodes, and finally arrive at the logic cells. For simplicity, we represent complex logic cells as a set of inverters. Each inverter has a P-type transistor of equivalent resistance R_{pi} and an N-type transistor of equivalent resistance R_{ni}. Their loads involving interconnect wires and driven cells are modeled as equivalent resistance R_i and capacitance C_i. When switch $\bar{G}_i$ (G_i) is on, the state transitions $0 \rightarrow 1$ ($1 \rightarrow 0$) will happen for these cells. Taking the former for example, we can obtain the currents at each power node according to Kirchhoff Circuit Laws, as shown in Equation (4).

$$I_{VDD} = \sum_{j=1}^{m} I_{VDD/Hj} = \sum_{j=1}^{m}\sum_{i=1}^{n} I_{VDD/Li} \\ \sum_{j=1}^{m}\sum_{i=1}^{n}[\frac{V_{VDD/Li} - V_{GND/Li}}{R_{pi} + R_i - 1/jwC_i} + I_{short} + I_{leak}] \quad (4)$$

where I_{short} and $I_{leakage}$ are the short-circuit current and static leakage current, respectively. From the above equation, we can find that currents that arose by transistor switching will assemble at the power grid in the upper metal layers.

The upper metal layers often have large dimensions. Meanwhile, hardware designers always insert metal fillers to meet the requirement of metal density. These metal fillers together with upper metal layers act as the metal shielding for the EM emanations from lower metal layers. During wave propagation, the reflection phenomenon occurs on the surface of metal shielding. We use the reflectivity of the surface to measure the amount of reflected radiation. This is defined as the ratio of the intensities of the reflected and incident radiation, and computed as Equation (5) for normal incidence ($\theta_{ic} = 0°$).

$$R = \frac{(1-\sqrt{2\varepsilon_0\omega/\sigma})^2+1}{(1+\sqrt{2\varepsilon_0\omega/\sigma})^2+1} \approx 1-\sqrt{2\varepsilon_0\omega/\sigma} \tag{5}$$

where the electrical conductivity σ of Cu approximates 5.7×10^7 S/m, vacuum permittivity approximates 8.85×10^{-12} F/m. The ω is circular frequency. A value of $R \approx 1$ means that most energy of EM fields is obstructed by upper metal shielding.

From the above analysis, we can deduce two claims about the underlying cause of ICs' EM emanations. Firstly, larger currents flow within the power grids in the upper metal layers as current accumulation. Then due to the existence of the metal shielding, EM emanations from lower metal layers hardly propagate to the external environment. This gives us the opportunity to reasonably simplify the EM simulation process. In EMSIM, various techniques, including device model approximation and parasitic network reduction, are leveraged to construct a simple but insightful model.

B. Parasitic Network Reduction

The modeling of the parasitic network is crucial during EM simulation. As shown in Figure 1 (a), in parasitic networks systems, metal wires are separated by vias and modeled as the combination of resistors (R) and capacitors (C). The values of these R and C components are obtained through parasitic extraction from the physical parameters, such as length, width and thickness, of metal wires. The inductance (L) of these components is optional due to the fact that inductive effects prevail gradually as the frequency increases [28]. As analyzed above, we focus on the EM emanations from the power grid in the upper metal layer.

The resulting questions are the simulation of currents flowing in these power grids. Previous EM simulations [8] exploit transistor-level Spice-like simulations on specified time frames. Interconnect wires are retained in this process as they provide input transition and load capacitance for the current analysis of transistor-level models. In our framework, we will predetermine the currents draw by each logic cell and thus exclude interconnect wires during final Spice-like simulations, a strategy to reduce the overall computational cost.

C. Device Model Approximation

Transistor-level models, typically specified in terms of mathematical equations, are required in existing EM simulation methods. Although with high accuracy, this type of model becomes impractical as the size of the circuits increases, so is the number of equations. Instead, we model each target logic cell as a current source with predetermined currents, as shown in Figure 1 (a). These currents are obtained through a cell-based, event-driven simulation, which links switching events to power currents through technology libraries provided by a foundry [29], [30]. The designer can also establish these technology libraries based on data from actual measurements or simulations [31]. Impedance results of the parasitic network are exploited to calculate the required input transition and load capacitance. The involved event-driven architecture computes power currents of logic cells only when their states change. This architecture facilitates the treatment between computational cost and simulation accuracy, due to the fact that switch activities of logic cells do not occur at regular time intervals. We then take these current profiles and use them to replace all logic cells in our Spice-style simulation with Piece-Wise Linear (PWL) current sources. This allows us to consider currents in logic cells in a less complex way.

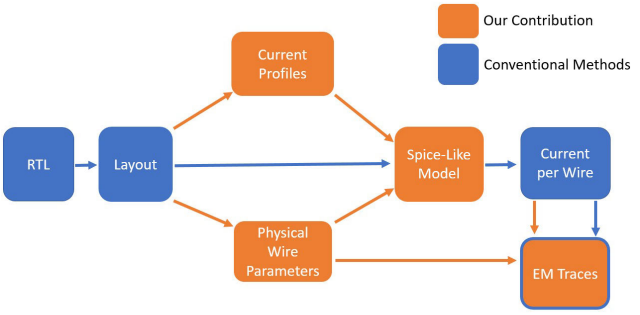


Fig. 2. The overall structure of EMSIM.

IV. EMSIM: FRAMEWORK

Based on the theoretical analysis, we will introduce the framework of EMSIM in this section. The overall structure of EMSIM is illustrated in Figure 2. It consists of three main steps: data preparation, current analysis and EM computation.

A. Data Preparation

A RTL-to-GDS flow is a prerequisite to creating a layout database, which provides input data for EMSIM. RTL descriptions are synthesized using specific technology libraries and then placed and routed. The layout database is created after geometry, connectivity and timing verification. This includes all GDSII data, layout-level netlists in Verilog, technology libraries, timing constraints and the timing data to specify interconnect delays and cell delays.

B. Current Analysis

We extract layout-level parasitics after passing layout versus schematic (LVS) checks. We use a commercial parasitic extractor, i.e., Calibre xRC, to calculate the parasitic resistance and capacitance of the physical layout. Note that other parasitic extractors can also be used in EMSIM. Through this we extract parasitics down to individual logic cells, while still preserving

the cell's internal structure and hierarchy. EMSIM performs parasitic network reduction to exclude interconnect wires from the parasitic netlist. This culminates in a reduced parasitic netlist which becomes part of the Spice model.

We then utilize device model approximation. First, we obtain the switching activities of logic cells. During the simulation, the layout-level netlist is annotated with the timing data and simulation model from a technology library. The switching activity from specific stimuli is recorded. EMSIM will only record the switching activities in given time intervals, over which we want to obtain EM emanations. This is realized by specifying constraints such as *dumpfile*, *dumpvars*, *dumpon* and *dumpoff* in Synopsys VCS [32]. Also, by allowing the user to choose logic cells to include in this simulation, we provide different levels of accuracy in the final results. The more logic cells included, the higher accuracy of the resulting simulation. As such, we include all logic cells although users of EMSIM may select a subset of cells. It is important to note that in side-channel security, lower accuracy denotes a stronger attacker rather than a weaker one, as logic cells that may generate noise or even actively defend the circuit are excluded. The reduced noise facilitates the process of security evaluation and vulnerability diagnosis, rather than obstructing it. As such, EMSIM provides flexible user modes for the security evaluation purpose.

Switching activity is combined with extracted parasitics and power information from the technology library to find the transient power of logic cells. The current profiles for each logic cell are obtained through dividing the transient power by the supply voltage. These current profiles complement the reduced parasitic netlist to form the combined Spice model.

Through hybridization, EMSIM combines a parasitic network model, current profiles, voltage and current source models, e.g., using modified nodal analysis (MNA) formulation, with circuit equations such as Kirchhoff's current and voltage laws to describe the physics and topology of a target circuit [33]. EMSIM uses the Spice-style simulator (e.g., HSpice [34]) to solve the transient current in each metal wire as a system of differential-algebraic equations (DAEs) with different initial conditions, e.g., plaintext and key for cryptographic circuits. HSpice uses direct linear solvers for the circuit system, which scales superlinearly with circuit sizes. Some improved tools, such as FastSPICE engines, can help accelerate the solution procedure.

C. Electromagnetic Computation

We approximate the magnetic field at a certain time, at a certain point ($B_{t,p}$) through Equation (6), similar to [7]. The explanation model is depicted in Figure 3. Note that x_i refers to the number of sub-regions in x and y_i the number of sub-regions in y for the i-th wire. Thus l_i and w_i are the length and width of the i-th wire's sub-regions. $r_{i,j,k,p}$ is the distance from the center of the sub-region to the measured point. $\hat{r}_{i,j,k,p}$ denotes its direction as a unit vector. $J_{i,t}$ is the current density in the i-th wire at time t, μ_0 is the magnetic permeability of free space. The total number of wires used for this step is determined by the structure of power grids in

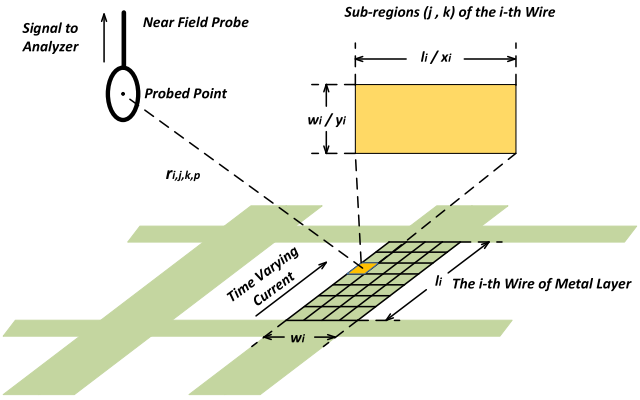


Fig. 3. The explanation model for EM computation.

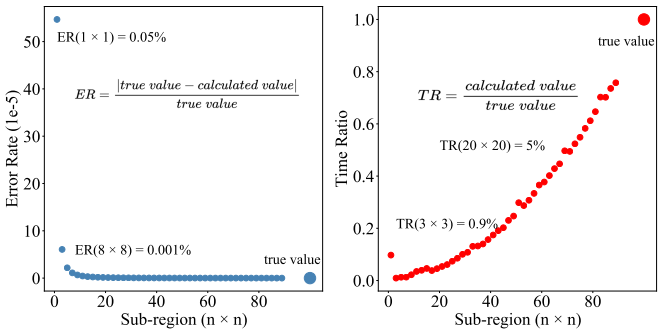


Fig. 4. The error rate (left) and time ratio (right) of different sub-regions division (wire parameters: $l = 10$ μm, $w = 5$ μm).

the upper metal layer, but not the overall circuit size. As the physical dimensions of metal wires are less than a tenth of their wavelength, we regard them as electrically small antennas with uniform current distribution. In this approximation, we divide the wire segment into a number of rectangular sub-regions of equal area. First, we multiply the area of each sub-region by the current in its wire. Second, we use the distance from the center of the sub-region to the simulated probe point to obtain the field of the sub-region on the target point. These effects are then summed through superposition to approximate the magnetic field at a certain point. It is important to note that the true value of the field is found by calculating the surface integral over the wire, instead of dividing the wire into sub-regions. Thus as the number of sub-regions increase, so does the simulation's accuracy.

$$B_{t,p} = \frac{\mu_0}{4\pi} \sum_{i \in wires} \sum_{j \in x_i} \sum_{k \in y_i} \frac{J_{i,t} \times \hat{r}_{i,j,k,p}}{r^2_{i,j,k,p}} l_i w_i \tag{6}$$

Take one metal wire as an instance, we divide the wire into various amounts of sub-regions and compute their results by discrete solution. The accuracy loss and time occupancy compared to true values are denoted as error rate (ER) and time ratio (TR) (see Figure 4). The error rate falls rapidly when increasing the amounts of sub-regions and is below 0.001 % starting from (8 × 8) sub-regions. The time ratio grows gradually and exceeds 5 % beginning with (20 × 20) sub-regions. EMSIM allows users to determine the amounts of sub-regions flexibly.

As the distances from each sub-region to a given point are constant, only $J_{i,t} \times \hat{r_{i,t}}$ need to be calculated for a given time in the simulation. The result of which is simply expanded by repetition into matrices and then multiplied by the distance matrix to find $B_{t,p}$. We use the NumPy library which provides multidimensional arrays to solve these matrices. Benefiting from large amounts of efficient cores, GPUs support parallel computing to accelerate the solving procedure. Still, numerical computations on GPUs are not supported in the NumPy library. This limits the computation speed as the size of solved matrices grows for large-scale circuits. Hence, we leverage GPU acceleration through the Numpy-compatible library CuPy. It is accelerated with the CUDA platform from NVIDIA and also uses CUDA-related libraries, including cuBLAS, cuDNN, cuRAND, cuSOLVER, cuSPARSE, and NCCL, to make full use of the GPU architecture [35], [36]. Since CuPy uses NumPy-style syntax, we can easily switch the computation modes between CPUs and GPUs based on the requirements.

In real measurements, the magnetic field is monitored through probes. Field changes in the loop surface S_{probe} of these probes induce a voltage signal, as written in Equation (7). For accuracy, the magnetic field at points as calculated by Equation (6) is converted to simulated probe voltage. EMSIM is a discrete-time simulation so we calculate the derivative of the magnetic field ($\frac{dB}{dt}$) according to Equation (8).

$$V_{probe} = -\int_{S_{probe}} \frac{dB}{dt} \cdot ds \tag{7}$$

$$x'(n) = \frac{x(n+1) - x(n-1)}{2} \tag{8}$$

The voltage signals from probes are typically weak and amplification is required for further processing. This is realized by the preamplifier integrated inside or outside probes, with a g dB amplification effect. The amplified signals V_{amp} calculated by Equation (9) will transmit to the front end of an oscilloscope or a spectrum analyzer. These reception devices allow voltage signals to pass through them at full amplitude until the harmonic frequency approaches the bandwidth limitation. EMSIM models the effect of bandwidth as a low-pass filter.

$$V_{amp} = 10^{\frac{g}{20}} \cdot V_{probe} \tag{9}$$

V. EMSIM VS EXISTING SOLUTIONS

To validate the feasibility of EMSIM in accurately and fast simulating the EM emanation of digital circuits, we designed a series of experiments. For the first step, we compare EMSIM results with other state-of-the-art approaches, in terms of intrinsic accuracy, application accuracy and computational cost with respect to time, frequency and spatial aspects, respectively. We then take the side-channel security evaluation as an instance and verify the application accuracy of EMSIM. These approaches (denoted as ConvEM in the paper) refer to EM simulations where transistor-level Spice-style simulations are used for current analysis where the CPU is used for calculation [8], [9].

A. Benchmark

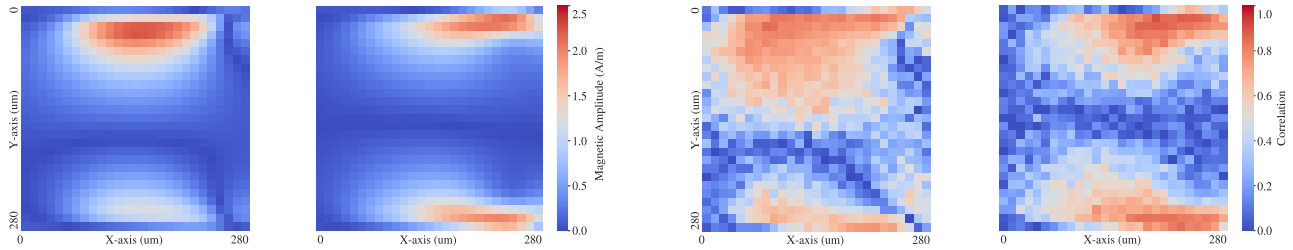
We select a 32-bit S-Box RTL design as the test object. The design is composed of four 8-bit S-Box modules and each one is realized in the form of the lookup table. An S-Box combines the multiplicative inverse with affine transformation, provides the nonlinearity to resist algebraic attacks. This design first goes through a RTL-to-GDS flow using 180 nm CMOS technology. The design consists of 900 cells and 31546 wires, and occupies 280.36 μm $\times$ 280.24 μm of die size. Following a typical design practice, we put the global power grids in metal layers M5 and M6, and local grids in the metal layer M1. The interconnect wires are distributed over all metal layers. We thus can reduce the number of wires for current analysis to 16070 through parasitic network reduction. In final EM computation, transient currents across 754 wires in the upper two layers are utilized. Its nominal supply voltage and the clock frequency are 1.8 V and 20 MHz, respectively. An XOR operation is first done between a secret key with plaintext, then delivered as the input data to the S-Box. For the final security evaluation, we assume that the adversary seeks to perform CEMA in order to recover the key.

B. Intrinsic Accuracy

We simulate currents in each wire under 100 input stimuli and then find EM emanations at the height of 30 μm above each intersection of a grid. Each box in this grid has a side length of about 10 μm. Each wire was divided down into 100 (10 $\times$ 10) sub-regions. Figure 5 (a) shows the magnetic map obtained by ConvEM and EMSIM at a specific time ($t = 26$ ns). The color bar quantifies the amount of magnetic amplitude, with blue being the lowest amplitude and red the highest. The magnetic amplitude as a function of location has a similar distribution between results from ConvEM and EMSIM. Computation results for SSIM metric show that their similarity is approximately 95%. Furthermore, the normalized magnetic waveforms at one position P_0 ($x = 175$ μm, $y = 15$ μm) are illustrated in Figure 6 (a), with a correlation exceeding 0.82. Also, their corresponding frequency domain signals are shown in Figure 6 (b), showing that the similarity reaches 0.63.

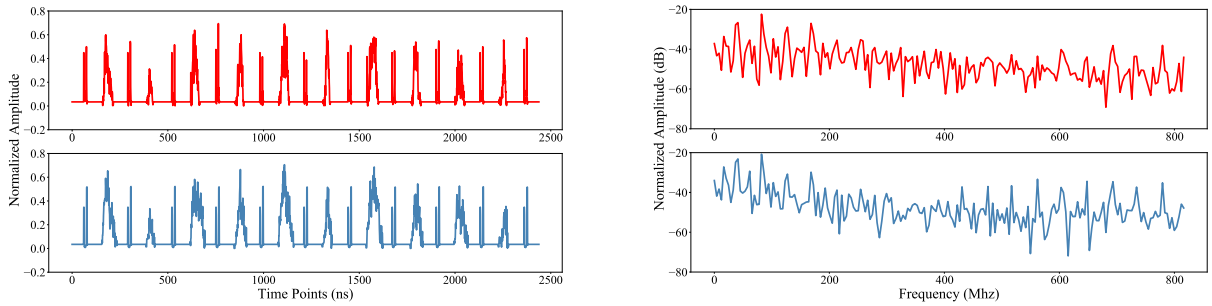
C. Application Accuracy

We then perform CEMA attacks on noisy traces of each position in the physical layout. Figure 5 (b) shows the correlation coefficients between EM traces and the correct key as a function of spatial locations. The color bar is used to quantify the degree of correlation leakage, in which the topmost color denotes that this point leaks maximum information that can be exploited by an attacker. The metric $ssim = 0.86$ indicates that the correlation leakage predicted by ConvEM and EMSIM has a similar spatial distribution. For position P_0, CEMA attack results are time series denoting the correlation between all traces and a certain key guess, as shown in Figure 7 (a). By taking the maximum across all the time series, we obtain the correct key. Results from ConvEM (top sub-figure) and EMSIM (bottom sub-figure) both demonstrate that the key



(a) magnetic map ($ssim = 0.95$) (b) correlation map ($ssim = 0.86$)

Fig. 5. The comparisons between ConvEM (left) and EMSIM (right).



(a) time domain traces ($ncc = 0.82$) (b) frequency domain traces ($ncc = 0.63$)

Fig. 6. The comparisons between ConvEM (top) and EMSIM (bottom).

TABLE II
REAL TIME SPENT ON EACH SIMULATION TIME POINT FOR A SIMPLE 32-BIT AES S-BOX

Method	Current Simulation	EM Computation
ConvEM	2.017 s	0.233 s
EMSIM	0.065 s	0.003 s

leaks at the time instant 26 ns with the peak value 0.82 of correlation traces. Figure 7 (b) and (c) illustrate the growth of the maximum correlations of different key guesses using an increasing number of traces N_{trace}. Among them, the red curve represents the correct guess of the secret key. Security analysis results show that we have MtD ≈ 7 for ConvEM and MtD ≈ 8 for EMSIM simulations, respectively.

D. Computation Cost

The computation time of EM simulation is compared in Table II between EMSIM and ConvEM. ConvEM requires a total simulation time of 2.25 s per time point, including 2.017 s for current analysis and 0.233 s for final EM computation. Correspondingly, EMSIM takes about 0.065 s and 0.003 s for the above steps, achieving facts of $\sim 31\times$ and $\sim 78\times$ speedup, respectively. Current simulation was ran on Intel X5690 (3.47 GHz). EM simulation was ran on a NVIDIA V100 GPU for EMSIM and Intel 9700k (4.6 GHz) for ConvEM.

VI. EMSIM VS SILICON MEASUREMENTS: AES S-BOX

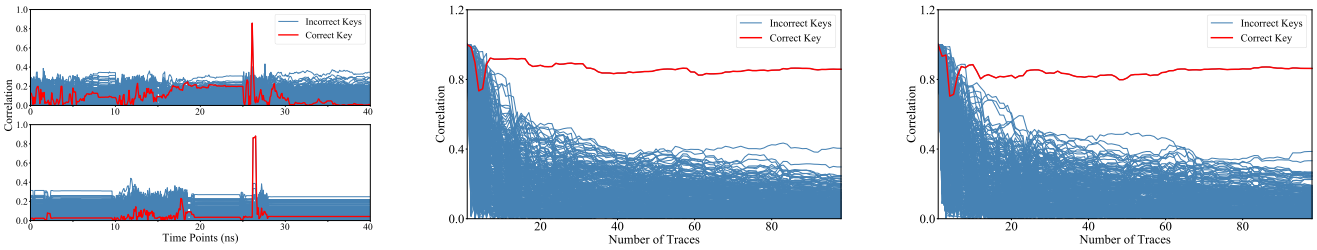
In order to compare the EMSIM simulation results with silicon measurements, we fabricated the 32-bit AES S-Box. Similar to Section V, comparisons are made for efficacy validation in terms of intrinsic accuracy and application accuracy.

A. Benchmark

Figure 8 (b) shows the physical layout of the 32-bit AES S-Box chip fabricated in a 180 nm CMOS technology. In addition to the S-Box circuit, we utilize a RS-232 serial communication block to make serial-parallel conversions. As a result, the number of the logic cells and metal wires increase to 1960 and 91985, respectively. We reduce the number of wires used in the current analysis to 56171 through parasitic network reduction. Only 668 transient currents across the upper two layers are considered in the EM computation. Each wire was divided down into 100 (10×10) sub-regions. The total chip occupies 790 μm$\times$750 μm and runs at 1.5 Mhz frequency. Other chip parameters like nominal supply voltage are kept the same as mentioned in Section V. In EM analysis attacks, an adversary prefers placing the EM probe as close as possible to the die surface so decapsulating the chip is often required. To better mimic this type of attack, we included an on-chip EM sensor placed at the topmost metal layer in the chip to collect EM traces. This sensor is a coil starting from the center, extending to the corners and covering the entire circuit [37], as shown in Figure 8 (b).

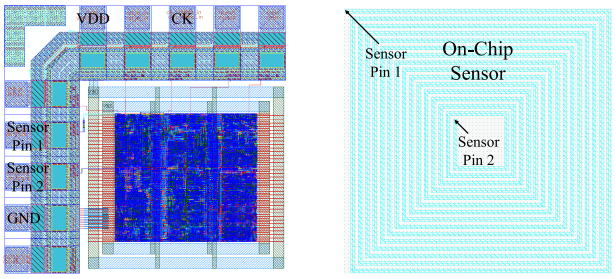
B. Analysis of Efficacy

1) Intrinsic Accuracy: During silicon measurements, we collect voltage signals from the on-chip sensor under 1000 input stimuli. The sampling rate is set as 2.5 GSa/s with 400 ps time interval. We take the average of 8 measurements (with the same 1000 input stimuli) aligned in the time domain through elastic alignment as the final data, to reduce the influence of external noise. EMSIM performs EM simulation to generate a 28×26 point grid under the same conditions. Then we acquire the voltage signals of the on-chip sensor by



(a) ConvEM (top) and EMSIM (bottom) (b) ConvEM (c) EMSIM

Fig. 7. CEMA attacks on the S-Box: correlation traces as a function of (a) time points and (b and c) stimuli number.



(a) chip layout (b) on-chip sensor

Fig. 8. Chip layout and on-chip sensor of the fabricated S-Box.

accumulating results of all the coils with gradually increasing diameters. Gaussian noise is added to mimic the effect of various noises on the final design. EMSIM takes about 1.192 s per time point in total, where 1.161 s is for current analysis and 0.031 s is for EM computation. Figure 9 (a) shows the EM traces obtained from silicon measurements (top sub-figure) and EMSIM results (bottom sub-figure), respectively. These traces are the function of time points under the stimuli, in which the output data of S-Box are stored in state registers. Using FFT, their spectrum distributions are computed and illustrated in Figure 9 (b). The EMSIM results match silicon measurements where $ncc = 0.74$ in the time domain and $ncc = 0.55$ in the frequency domain. Note that the noise components in the frequency spectrum lead to the decline of similarity.

2) Application Accuracy: Finally, CEMA attacks are carried out on traces from both the silicon measurement and EMSIM simulation results. The correlation traces changing with time series are illustrated in Figure 10 (a). The maximum correlations of the correct key are 0.21 and 0.23 for silicon measurement (top sub-figure) and EMSIM simulation (bottom sub-figure). As the on-chip sensor covers positions carrying low correlation leakage, this leads to lower correlation coefficients compared to results from Section V. Moreover, they have a similar leakage time interval, where the correlations from the correct key exceed those from incorrect keys. Figure 10 (b) and Figure 10 (c) depicts the growth of the maximum correlations of different key guesses using an increasing number of traces. As shown in the figure, we have MtD $\approx$ 185 for silicon measurements and MtD $\approx$ 162 for EMSIM simulations. This means that EMSIM results align with real silicon measurements from the perspective of security evaluation.

TABLE III
REAL TIME SPENT ON EACH SIMULATION TIME POINT FOR A CIRCUIT WITH RS-232 IN ADDITION TO A 32-BIT AES S-BOX

Method	Current Simulation	EM Computation
EMSIM	1.161 s	0.031 s

VII. EMSIM VS SILICON MEASUREMENTS: AES-128

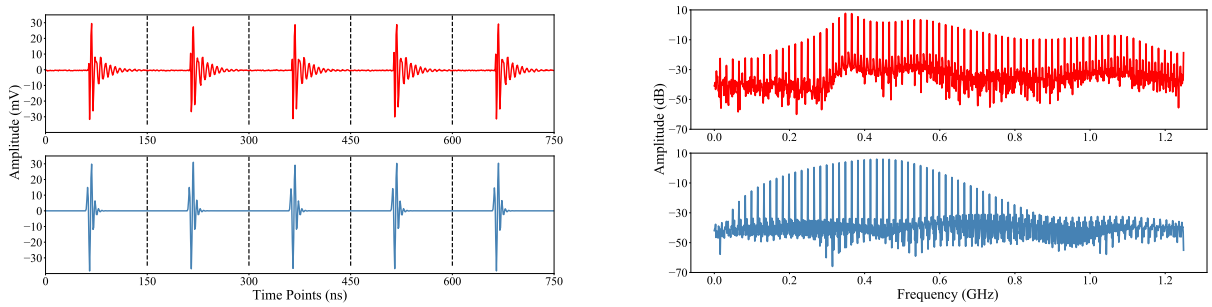
Besides the previous experiments, we try to validate the efficacy of EMSIM on large designs under the same aspects of comparison. To achieve this goal, we design and fabricate a 128-bit AES design (denoted as AES-128 in the paper). Our experimental result will further prove the scalability of the developed EMSIM.

A. Experimental Setup

We set up the near-field scanner system to collect the EM signals from chips, as illustrated in Figure 11. The system consists of a microscope camera, three-axis positioning platform, near-field microprobe, oscilloscope, shielding box and PC. The ICR HH250-75 near-field microprobe is used, with a resolution of 150 um. The magnetic fields are collected by its horizontal measuring coil and amplified using the internal preamplifier up to +30 dB magnification. The microprobe is placed at the close vicinity of the IC surface. During measurement, We first select the reference coordinate of near-field scanning based on the die image captured by the microscope camera. Then the probe is controlled using the three-axis positioning platform to finish the near-field scanning targeted on the IC surface. The collected magnetic fields are transmitted through an oscilloscope to the PC for the consequent process. All the equipment used for magnetic field collection is placed in a shielding box to reduce environmental noise.

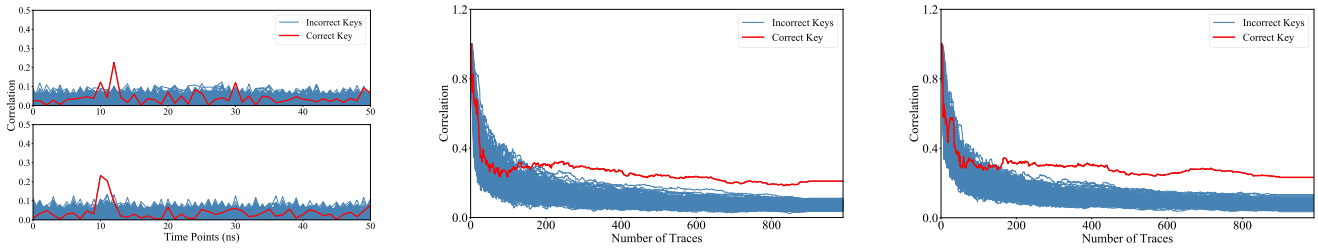
B. Benchmark

As shown in Figure 12 (a), the AES-128 design [38] executes the KeyExpansion operation first and then ten rounds of encryptions. Among them, the top nine rounds of encryption execute SubBytes, ShiftRows, Mixcolumns and AddRoundKey operations in succession. While the last round of encryption does not execute the Mixcolumns operation. In each round, the SubBytes operation occupies the four clock cycles and other operations take up the follow-up one cycle. Intermediate data and final output data from these operations are



(a) time domain ($ncc = 0.74$) (b) frequency domain ($ncc = 0.55$)

Fig. 9. The comparisons of EM signals obtained by silicon measurements (top) and EMSIM results (bottom).



(a) silicon (top) and EMSIM results (bottom) (b) silicon measurements (c) EMSIM results

Fig. 10. CEMA attacks on the fabricated S-Box: correlation traces as a function of (a) time points and (b and c) stimuli number.

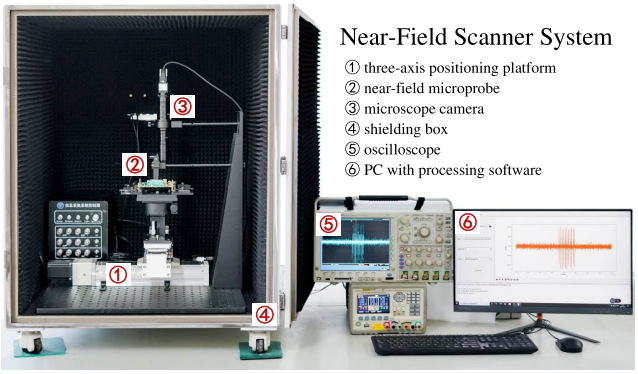


Fig. 11. The overview of the experimental setup.

stored and transmitted using state registers. We apply the RTL-to-GDS flow technology to implement the AES-128 design using 180 nm CMOS technology. The final layout contains 14559 gates with 733662 metal wires, and the global power grids occupy the metal layers M5 and M6. Figure 12 (b) shows the die image of the fabricated AES-128 with 1.6 mm×1.3 mm die area. Its supply voltage and clock frequency are set as 1.8 V and 25 Mhz, respectively. During silicon measurements, the fixed key and 1000 random input stimuli are delivered to the AES-128 chip for data encryption. In this process, we collect the EM signals emanated from the vicinity of the chip surface. The scan grid overlay (22 × 12 points) is also depicted in Figure 12 (b). Total 26400 traces are acquired for the fabricated AES-128 design, under 2.5 GSa/s sampling rate. Then we take the average of 32 measurements (with the same 1000 input stimuli) aligned in the time domain through elastic alignment as the final data. When predicting the EM emanations, EMSIM will reduce the number of wires to 365529 for current analysis and 1424 for electromagnetic computation. Each wire was divided down into 100 sub-regions. Other simulation settings are kept in the same condition as the silicon measurements. EMSIM takes about 3.860 s per time point in total, where 3.451 s is for current analysis and 0.409 s is for EM computation.

C. Analysis of Efficacy

1) Intrinsic Accuracy: Based on the results from silicon measurement and EMSIM, we build the map of EM signals for one specific time ($t = 1356.4$ ns) from the chip surface. The comparison is illustrated in Figure 13. This specific time locates in the clock cycle where the AES-128 executes the SubByte operation targeting on the first four bytes. The magnetic amplitude as a function of location has a similar distribution between results from silicon measurement and EMSIM ($ssim = 0.98$). Specifically, the lowest amplitude (negative axis) and highest amplitude (positive axis) occur at the top left corner and top right corner of the chip surface. When the probe moves from left to right side, the amplitude of EM signals will first decrease along the negative axis and then increase along the positive axis. Hence the boundary between negative and positive axes appears on the map of EM signals. These two boundaries built by EMSIM and silicon measurements have a similar trend. Moreover, we compare the simulated results with the real signals detected by the EM probe, where Figure 14 (a) shows one position P_1 ($x = 25$ μm, $y = 475$ μm) and Figure 14 (b) show another position P_2 ($x = 475$ μm, $y = 225$ μm). These figures depict the varying signals during the complete encryption of AES-128. As shown in the figure, the experimental results obtained from silicon measurements and EMSIM have similar

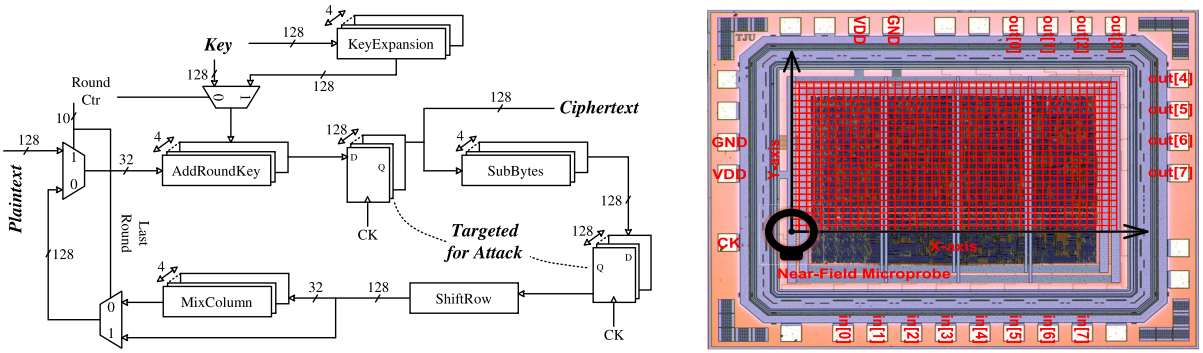
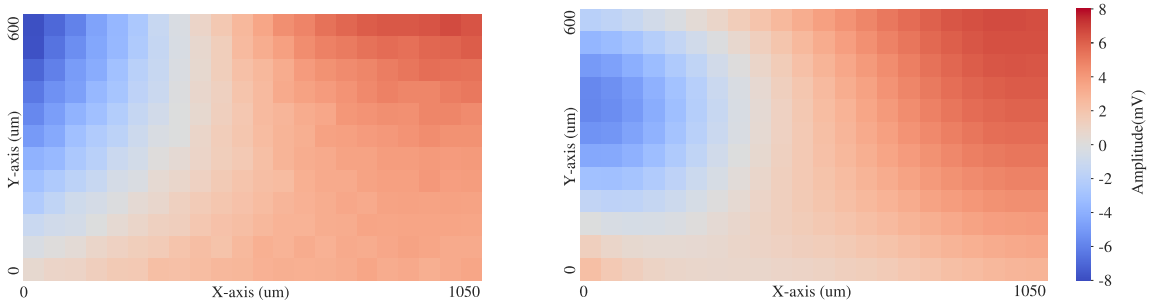


Fig. 12. The hardware architecture (left) and die image (right) of the fabricated AES design.



(a) silicon measurements (b) EMSIM results

Fig. 13. The map of EM signals obtained by silicon measurements and EMSIM results ($ssim = 0.98$).

amplitude range at different positions. The similarity ncc reaches 0.85 and 0.74 at the above positions, respectively. We then transform the EM signals from the time domain to the frequency domain. As shown in Figure 15, signal peaks of both amplitude spectra occur at frequency points 25 MHz and 50 MHz. Note that they are the fundamental frequency and the first harmonic frequency of the AES-128 circuit. For position P_1 and P_2, frequency spectra obtained from EMSIM have similarity $ncc = 0.57$ and $ncc = 0.52$ with those from silicon results, respectively. Note that the noise components in the frequency spectrum lead to the decline of similarity.

2) Application Accuracy: CEMA attacks are performed on EM traces detected from each position of the chip surface. We chose the time window where SubBytes operation of the first four bytes as the attack target. Figure 16 demonstrates the attack results on the EM signals obtained from silicon measurements. Among them, Figure 16 (a) shows the correlation coefficients between EM traces and the correct key as a function of spatial locations. It indicates that the top left corner and top right corner of the chip surface have a higher possibility to leak sensitive information. Further, we depict the correlation traces as a function of stimuli number in Figure 16 (b) and Figure 16 (c), respectively. For the position P_1, the maximum correlation of the correct key is 0.25 and its MtD $\approx$ 244. For the position P_2, the attacker can not reveal the correct key after 1000 traces, since its maximum correlation 0.13 is submerged by those of other guessed keys. We also demonstrate the attack results on the EM signals obtained from EMSIM tool in Figure 17. As shown, the map of correlation coefficients has a similar distribution compared to the result from silicon measurements ($ssim = 0.93$). At position P_1, we have MtD $\approx$ 150 with the maximum correlation $\approx$ 0.30. Correspondingly, the attacker cannot recover the correct key at the position P_2, since the correlation coefficient reaches only 0.13 using 1000 traces. All of these comparisons mean that EMSIM results align with real silicon measurements from the security evaluation perspective.

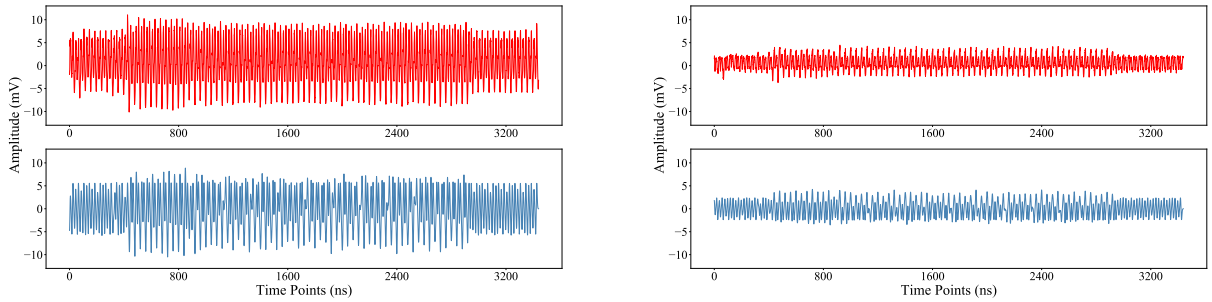
VIII. EMSIM: APPLICATIONS

In this section, we demonstrate application cases of EMSIM that examine security flaws and assist in protection schemes. Two types of countermeasures on AES-128 design are tested including masking schemes and physical strategies. Also, we show the possibility that incorporating EMSIM with existing field solvers such as Ansys HFSS.

A. Verification for Masking Schemes

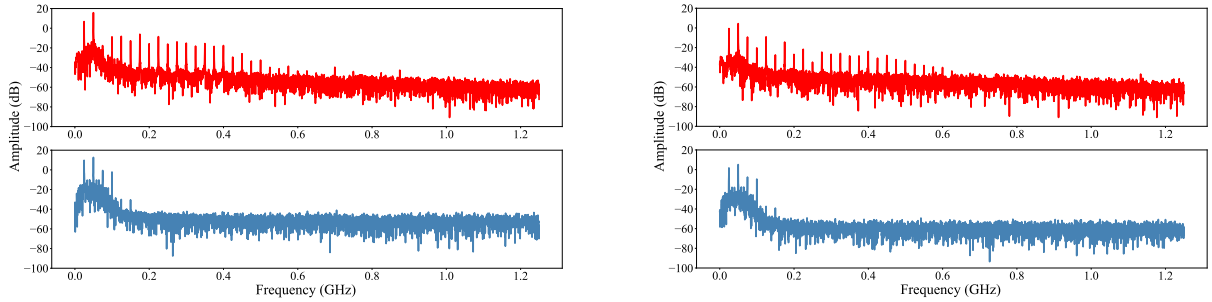
The masking scheme proposed by Oswald et al. [39] is an algorithm-level countermeasure against first-order SCA attacks. The core idea is to split sensitive variables into several shares and import them to circuit operations separately. Although this scheme is provably secure in theory, previous works [40], [41] have found that glitches in masked AES chip limit its practical effects. The security flaw is ascribed to the switching properties of XOR cells in masked multipliers. Here we draw similar conclusions using EMSIM before manufacturing. EMSIM partitions the chip surface into a 23×17 point grid and measures EM emanations at the height of 30 μm.

As a comparison, we first perform Attack 1 on 10000 simulated traces based on the Hamming weight model of output states. Then a toggle-count model of masked AES S-Box is



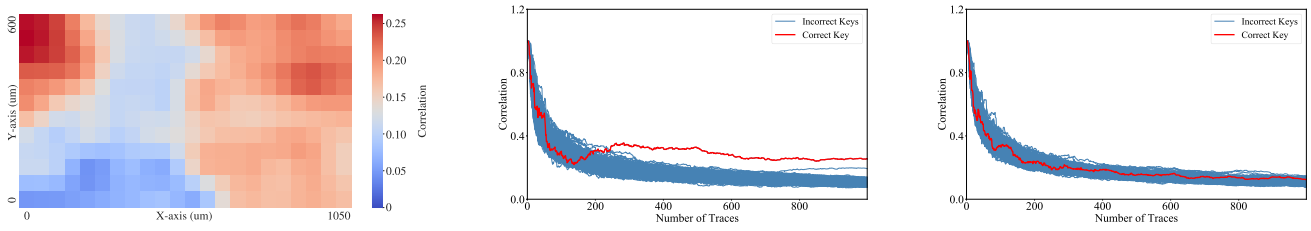
(a) position P_1 ($ncc = 0.85$) (b) position P_2 ($ncc = 0.74$)

Fig. 14. The comparisons of EM signals obtained by silicon measurements (top) and EMSIM results (bottom).



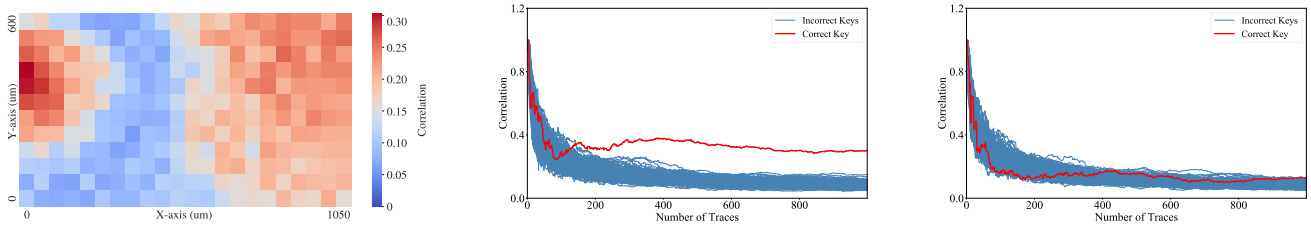
(a) position P_1 ($ncc = 0.57$) (b) position P_2 ($ncc = 0.52$)

Fig. 15. The comparisons of EM spectrum obtained by silicon measurements (top) and EMSIM results (bottom).



(a) spatial locations (b) position P_1 (c) position P_2

Fig. 16. Actual CEMA attacks on the fabricated AES-128: (a) correlation of the correct key as a function of (a) spatial locations and stimuli number for (b) position P_1 and (c) position P_2.



(a) spatial locations (b) position P_1 (c) position P_2

Fig. 17. Simulated CEMA attacks on the fabricated AES-128: correlation of the correct key as a function of (a) spatial locations and stimuli number for (b) position P_1 and (c) position P_2.

adopted in Attack 2. This model was created by counting the average number of transitions occurring in masked AES S-Box under different data inputs. Locations with maximum ρ_{max} of the correct key are selected for security comparison. Figure 18 shows the attack results obtained from Hamming weight model and toggle-count model. In Attack 1, some wrong key candidates lead to significant peaks in the correlation traces. While in Attack 2, the correct key byte (8'h23) is obviously discernible from all false-guessed keys. Hence designers can examine whether countermeasures exist security flaws at the phase of hardware implementation, with the support of EMSIM.

B. Verification for Physical Strategies

Physical strategies prefer securing circuit designs at logic and circuit level, involving secure logic styles [42], current signature attenuation [12] and metal layer redesigning [43],

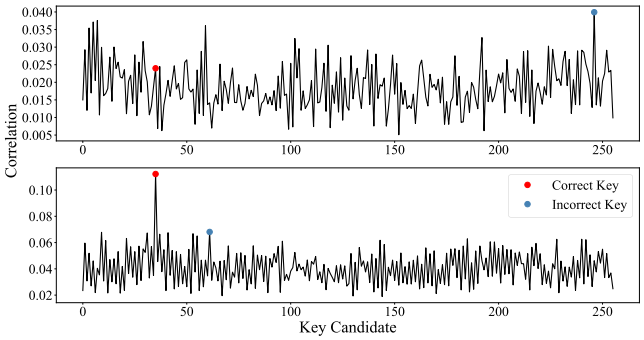
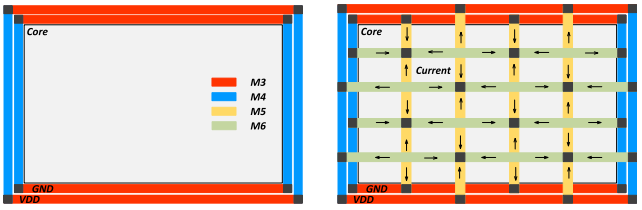


Fig. 18. Results comparison between Hamming weight model (top) and toggle-count model (bottom).



(a) Design 1 (b) Design 2

Fig. 19. AES-128 designs with different power grids.

TABLE IV
COMPARISON BETWEEN DESIGN STRATEGIES

Design #	Design Strategy	Max. Correlation	Min. MtD
Design 1	Baseline Design	0.43	≈ 100
Design 2	Four set of power stripes	0.12	> 1000

etc. Among them, metal layer redesigning often optimizes the power grids to decrease sensitive information leaked by metal wires. This type of strategy has been analyzed and validated in several previous works [8], [15], [43]. With support from EMSIM, we further investigate the impact of power stripes (VDD and GND) settings on the EM SCA resistance of ICs.

Figure 19 shows AES-128 designs with two different power grids. The baseline AES-128 is implemented using M1-M4 metal layers, denoted as Design 1. Upon the baseline design, Design 2 adds two sets of vertical power stripes in the M5 layer and two sets of horizontal power stripes in the M6 layer. These power stripes are uniformly distributed with 40 μm width. Other chip parameters and simulation settings are kept the same as mentioned in Section VII. EMSIM partitions the chip surface into a 23×17 point grid and finds EM emanations at the height of 30 μm. We select locations with maximum ρ_{max} and minimum MtD for security comparison. Table IV demonstrates that Design 2 has higher resistance against EM analysis attacks. This attributes to the following two reasons. Robust power grids with more power stripes will lead to lower currents flowing with metal wires. Meanwhile, EM emanations produced by power grids cancel out each other partially. Figure 19 (b) marks current directions across power stripes. We can redesign and evaluate power grids iteratively until satisfying security and other requirements. Hence, EMSIM can provide pre-silicon verification for EM side-channel security, assist designers in more secure physical design strategies.

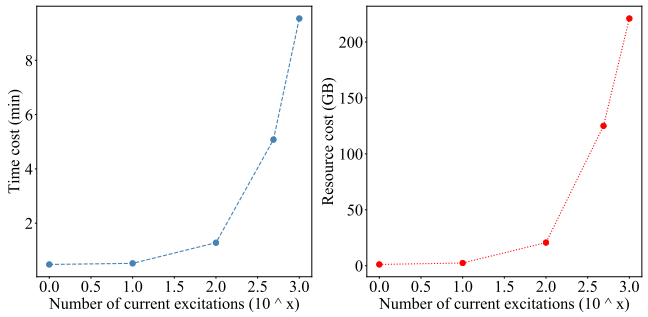


Fig. 20. The time (left) and resource (right) of the HFSS-based framework.

C. Scalability to HFSS-Based Framework

As discussed in Section II-A, existing field solvers such as Ansys HFSS are not adapted for simulating EM simulation of ICs. They confront the following two challenges. First, as complex nanometer-scale objects, the setup and analysis of model solutions consume enormous time and resources. Second, there lack of excitations to simulate transient behaviors of CMOS logic cells. Up to now, we have not found any HFSS-based frameworks used for pre-silicon EM security evaluation. Only authors in [44] and [12] build a simplified model (9 wires connected with 8 vias) using HFSS to investigate the EM propagation within ICs.

As a result, in order to address the reviewer's comment, we propose an HFSS-based framework to simulate time-domain EM emanations from ICs ourselves, based on our EMSIM framework. This HFSS-based framework is comprised of several steps. In Step 1, we construct the 3D metal-layer model in HFSS based on the GDSII data of design. This model excludes interconnect wires through parasitic network reduction. In Step 2, we model each target logic cell as a whole with predetermined currents. This is achieved by device model approximation. These currents are exploited to replace all logic cells, in the form of current excitations. In Step 3, we simulate the EM emanations from the design with the HFSS transient solver. Though theoretically possible, the HFSS-based framework does not support EM simulations for complex circuits such as AES-128. Figure 20 records the time and resource cost as current excitations increase ran on Intel Xeon E5-2670 v2 CPU with 256 GB RAM. The complete AES-128 with 14559 logic cells will occupy 3.14 TB of memory and take more than 2.31 h just to save fields per sample point. It is apparent that this HFSS-based framework needs more optimizations to make it more practical. It may be a future direction of work but needs collaboration with the industry as HFSS is a commercial tool.

IX. CONCLUSION

In this paper, we develop the EMSIM framework to significantly speed up EM simulation at the layout level, making pre-silicon EM verification for larger-scale circuits practical. To achieve this goal, we implement multiple techniques, including device model approximation and parasitic network reduction for the current analysis and GPU acceleration for EM computation. These simulated EM traces can be used for design-time checking with respect to functional safety as

well as information security. The effectiveness of EMSIM is validated in terms of intrinsic accuracy, computation time and final application evaluation results.

REFERENCES

[1] M. Ramdani et al., "The electromagnetic compatibility of integrated circuits—Past, present, and future," *IEEE Trans. Electromagn. Compat.*, vol. 51, no. 1, pp. 78–100, Feb. 2009.

[2] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proc. Annu. Int. Cryptol. Conf.* Berlin, Germany: Springer, 1999, pp. 388–397.

[3] H. Yu, H. Ma, K. Yang, Y. Zhao, and Y. Jin, "DeepEM: Deep neural networks model recovery through EM side-channel information leakage," in *Proc. IEEE Int. Symp. Hardw. Oriented Secur. Trust (HOST)*, Dec. 2020, pp. 209–218.

[4] M. P. Babitha and K. R. R. Babu, "Secure cloud storage using AES encryption," in *Proc. Int. Conf. Autom. Control Dyn. Optim. Techn. (ICACDOT)*, Sep. 2016, pp. 859–864.

[5] Ansys. *Ansys HFSS*. Accessed: Aug. 2, 2021. [Online]. Available: https://www.ansys.com/products/electronics/ansys-hfss

[6] H. Li, A. T. Markettos, and S. Moore, "Security evaluation against electromagnetic analysis at design time," in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst.* Berlin, Germany: Springer, 2005, pp. 280–292.

[7] V. Lomné, P. Maurine, L. Torres, T. Ordas, M. Lisart, and J. Toublanc, "Modeling time domain magnetic emissions of ICs," in *Proc. Int. Workshop Power Timing Modeling, Optim. Simulation*. Berlin, Germany: Springer, 2010, pp. 238–249.

[8] A. Kumar, C. Scarborough, A. Yilmaz, and M. Orshansky, "Efficient simulation of EM side-channel attack resilience," in *Proc. IEEE/ACM Int. Conf. Comput.-Aided Design (ICCAD)*, Nov. 2017, pp. 123–130.

[9] H. Ma, J. He, Y. Liu, Y. Zhao, and Y. Jin, "CAD4EM-P: Security-driven placement tools for electromagnetic side channel protection," in *Proc. Asian Hardw. Oriented Secur. Trust Symp. (AsianHOST)*, Dec. 2019, pp. 1–6.

[10] S. van der Walt, S. C. Colbert, and G. Varoquaux, "The NumPy array: A structure for efficient numerical computation," *Comput. Sci. Eng.*, vol. 13, no. 2, pp. 22–30, 2011.

[11] R. Nishino and S. H. C. Loomis, "CuPy: A numpy-compatible library for NVIDIA GPU calculations," *Proc. 31st Conf. Neural Inf. Process. Syst.*, 2017, vol. 151, no. 7, pp. 1–7.

[12] D. Das, M. Nath, B. Chatterjee, S. Ghosh, and S. Sen, "STELLAR: A generic EM side-channel attack protection through ground-up root-cause analysis," in *Proc. IEEE Int. Symp. Hardw. Oriented Secur. Trust (HOST)*, May 2019, pp. 11–20.

[13] J. He, H. Ma, X. Guo, Y. Zhao, and Y. Jin, "Design for EM side-channel security through quantitative assessment of RTL implementations," in *Proc. 25th Asia South Pacific Design Autom. Conf. (ASP-DAC)*, Jan. 2020, pp. 62–67.

[14] E. Peeters, F. X. Standaert, and J. J. Quisquater, "Power and electromagnetic analysis: Improved model, consequences and comparisons," *Integr. VLSI J.*, vol. 40, no. 1, pp. 52–60, Jan. 2007.

[15] D. Poggi, T. Ordas, A. Sarafianos, and P. Maurine, "Checking robustness against EM side-channel attacks prior to manufacturing," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 41, no. 5, pp. 1264–1275, May 2022.

[16] T. Ordas, M. Lisart, E. Sicard, P. Maurine, and L. Torres, "Near-field mapping system to scan in time domain the magnetic emissions of integrated circuits," in *Proc. Int. Workshop Power Timing Modeling, Optim. Simulation*. Berlin, Germany: Springer, 2008, pp. 229–236.

[17] S. Banik, A. Bogdanov, and F. Regazzoni, "Atomic-AES: A compact implementation of the AES encryption/decryption core," in *Proc. Int. Conf. Cryptol. India*. Cham, Switzerland: Springer, 2016, pp. 173–190.

[18] J.-J. Quisquater and D. Samyde, "Electromagnetic analysis (EMA): Measures and counter-measures for smart cards," in *Proc. Int. Conf. Res. Smart Cards*. Berlin, Germany: Springer, 2001, pp. 200–210.

[19] N. Sehatbakhsh, B. B. Yilmaz, A. Zajic, and M. Prvulovic, "EMSim: A microarchitecture-level simulation tool for modeling electromagnetic side-channel signals," in *Proc. IEEE Int. Symp. High Perform. Comput. Archit. (HPCA)*, Feb. 2020, pp. 71–85.

[20] D. McCann, E. Oswald, and C. Whitnall, "Towards practical tools for side channel aware software engineering: 'Grey box' modelling for instruction leakages," in *Proc. 26th USENIX Secur. Symp. (USENIX Secur.)*, 2017, pp. 199–216.

[21] A. Tsukioka et al., "A fast side-channel leakage simulation technique based on IC chip power modeling," *IEEE Lett. Electromagn. Compat. Pract. Appl.*, vol. 1, no. 4, pp. 83–87, Dec. 2019.

[22] N. Veshchikov, "SILK: High level of abstraction leakage simulator for side channel analysis," in *Proc. 4th Program Protection Reverse Eng. Workshop*, 2014, pp. 1–11.

[23] H. Ma, J. He, M. Panoff, Y. Jin, and Y. Zhao, "Automatic on-chip clock network optimization for electromagnetic side-channel protection," *IEEE J. Emerg. Sel. Topics Circuits Syst.*, vol. 11, no. 2, pp. 371–382, Jun. 2021.

[24] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," *IEEE Trans. Image Process.*, vol. 13, no. 4, pp. 600–612, Apr. 2004.

[25] T. Schneider and A. Moradi, "Leakage assessment methodology," in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst.* Springer, 2015, pp. 495–513.

[26] C. Whitnall and E. Oswald, "A cautionary note regarding the usage of leakage detection tests in security evaluation," Int. Assoc. Cryptolog. Res., Tech. Rep. 2019/703, 2019.

[27] S. K. Rao, D. Krishnankutty, R. Robucci, N. Banerjee, and C. Patel, "Post-layout estimation of side-channel power supply signatures," in *Proc. IEEE Int. Symp. Hardw. Oriented Secur. Trust (HOST)*, May 2015, pp. 92–95.

[28] I. P. Vaisband, R. Jakushokas, M. Popovich, A. V. Mezhiba, S. Köse, and E. G. Friedman, *On-Chip Power Delivery and Management*. Springer, 2016.

[29] C. Knoth, H. Jedda, and U. Schlichtmann, "Current source modeling for power and timing analysis at different supply voltages," in *Proc. Design, Automat. Test Eur. Conf. Exhib. (DATE)*, Mar. 2012, pp. 923–928.

[30] M. S. Abrishami, M. Pedram, and S. Nazarian, "CSM-NN: Current source model based logic circuit simulation—A neural network approach," in *Proc. IEEE 37th Int. Conf. Comput. Design (ICCD)*, Nov. 2019, pp. 393–400.

[31] M. M. Sharifi et al., "A novel TIGFET-based DFF design for improved resilience to power side-channel attacks," in *Proc. DATE*, 2020, pp. 1253–1258.

[32] Synopsys. *VCS*. Accessed: Aug. 2, 2021. [Online]. Available: https://www.synopsys.com/verification/simulation/vcs.html

[33] M. Rewieński, "A perspective on fast-SPICE simulation technology," in *Simulation and Verification of Electronic and Biological Systems*. Dordrecht, The Netherlands: Springer, 2011, pp. 23–42.

[34] Synopsys. *HSPICE*. Accessed: Aug. 2, 2021. [Online]. Available: https://www.synopsys.com/zh-cn/verification/ams-verification/hspice.html

[35] S. Tokui et al., "Chainer: A deep learning framework for accelerating the research cycle," in *Proc. 25th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, 2019, pp. 2002–2011.

[36] J. M. Morton et al., "DelayRepay: Delayed execution for kernel fusion in Python," in *Proc. 16th ACM SIGPLAN Int. Symp. Dyn. Lang.*, 2020, pp. 43–56.

[37] J. He, X. Guo, H. Ma, Y. Liu, Y. Zhao, and Y. Jin, "Runtime trust evaluation and hardware trojan detection using on-chip EM sensors," in *Proc. 57th ACM/IEEE Design Autom. Conf. (DAC)*, Jul. 2020, pp. 1–6.

[38] Secworks. (2014). *NIST Document FIPS 197 Based AES Design*. [Online]. Available: https://github.com/secworks/aes

[39] E. Oswald, S. Mangard, N. Pramstaller, and V. Rijmen, "A side-channel analysis resistant description of the AES S-box," in *Proc. Int. Workshop Fast Softw. Encryption*. Berlin, Germany: Springer, 2005, pp. 413–423.

[40] S. Mangard, N. Pramstaller, and E. Oswald, "Successfully attacking masked AES hardware implementations," in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst.* Berlin, Germany: Springer, 2005, pp. 157–171.

[41] S. Mangard and K. Schramm, "Pinpointing the side-channel leakage of masked AES hardware implementations," in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst.* Berlin, Germany: Springer, 2006, pp. 76–90.

[42] K. Tiri and I. Verbauwhede, "A VLSI design flow for secure side-channel attack resistant ICs," in *Proc. Design, Autom. Test Eur.*, 2005, pp. 58–63.

[43] M. Wang et al., "Physical design strategies for mitigating fine-grained electromagnetic side-channel attacks," in *Proc. IEEE Custom Integr. Circuits Conf. (CICC)*, Apr. 2021, pp. 1–2.

[44] A. W. Khan, T. Wanchoo, G. Mumcu, and S. Kose, "Implications of distributed on-chip power delivery on EM side-channel attacks," in *Proc. IEEE Int. Conf. Comput. Design (ICCD)*, Nov. 2017, pp. 329–336.

Haocheng Ma received the B.S. degree in microelectronics from Tianjin University, Tianjin, China, in 2017, where he is currently pursuing the Ph.D. degree with the School of Microelectronics. His current research interests include digital circuit design, hardware security, and EDA for security.

Max Panoff (Graduate Student Member, IEEE) received the B.E. degree in electrical engineering from the Stevens Institute of Technology, Hoboken, NJ, USA, in 2018. He is currently pursuing the Ph.D. degree in electrical engineering with the University of Florida. His research interests include hardware security, especially side channel analysis.

Jiaji He received the B.S. degree in electronic science and technology and the M.S. and Ph.D. degrees in microelectronics from Tianjin University in 2013, 2015, and 2019, respectively. He was a Visiting Scholar at UCF and UF from 2016 to 2018. He was a Post-Doctoral Research Fellow at the Institute of Microelectronics, Tsinghua University, from 2019 to 2021, where he is currently an Associate Professor. His research interests include digital circuit design, hardware security, and EDA for security.

Yiqiang Zhao (Member, IEEE) received the B.S. degree in semiconductor physics and device, the M.S. degree in microelectronics, and the Ph.D. degree in microelectronics and solid-state electronics from Tianjin University, Tianjin, China, in 1988, 1991, and 2006, respectively.

In 1991, he joined the Jinhang Technical Physics Institute, Tianjin, where he was responsible for analog and mixed signal circuit design. Since 2001, he has been with the School of Electronic Information Engineering and the School of Microelectronics, Tianjin University, where he is currently a Professor. His research interests include mixed-signal integrated circuits, security chips, and hardware security.

Yier Jin (Senior Member, IEEE) received the B.S. and M.S. degrees in electrical engineering from Zhejiang University, China, in 2005 and 2007, respectively, and the Ph.D. degree in electrical engineering from Yale University in 2012. He is an Associate Professor and the Warren B. Nelms IoT Term Professor with the Department of Electrical and Computer Engineering (ECE), University of Florida (UF). His research interests include hardware security, embedded systems design and security, trusted hardware intellectual property (IP) cores, hardware-software co-design for modern computing systems, and security analysis on the Internet of Things (IoT) and wearable devices with particular emphasis on information integrity and privacy protection in the IoT era.