CAD4EM-P: Security-Driven Placement Tools for Electromagnetic Side Channel Protection

Haocheng Ma*, Jiaji He†, Yanjiang Liu*, Yiqiang Zhao* and Yier Jin‡
*School of Microelectronics, Tianjin University, Tianjin 300072, China
†Institute of Microelectronics, Tsinghua University, Beijing 100084, China
‡Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL 32611, USA
hc_ma@tju.edu.cn, jiaji_he@mail.tsinghua.edu.cn, yanjiang_liu@tju.edu.cn, yq_zhao@tju.edu.cn, yier.jin@ece.ufl.edu

***Abstract*—Side-Channel Analysis (SCA) attacks are major threats to hardware security. Upon this security threat, various countermeasures at different design layers have been proposed against SCA attacks. These approaches often introduce significant performance overheads and impose high requirements of side-channel security backgrounds to IC designers. In this paper, we propose an automatic computer-aided design (CAD) tool that can enhance the circuit resistance against electromagnetic (EM) SCA attacks. This new tool will guide a security-driven placement process and can be seamlessly integrated into the modern IC design flow. The protected IC design will be resilient to SCA attacks with negligible area and power overheads. In order to develop this tool, we first investigate the root-cause of EM leakage at layout level and mathematically demonstrate the feasibility of security-driven placement through the EM leakage modeling. We then identify that the correlation between the data under protection and the EM leakage can be significantly reduced through data-dependent registers reallocation. Simulation results on cryptographic circuits prove the effectiveness of both the constructed EM leakage model and the EM model based CAD tool for EM security.**

***Index Terms*—CAD for Security, Side-Channel Attack, Electromagnetic Leakage, Placement**

I. Introduction

CAD tools play important roles in modern integrated circuits (ICs) development, with the aim of cost reduction, design automation and performance enhancement. CAD tools facilitate the IC design process from the behavioral specification to the ultimate physical design. Among them, *Synthesis* tools convert the circuit RTL description into a gate-level netlist based on a selected technology library. *Floorplanning* tools help arrange circuit components and gates in the form of rectangular blocks. *Placement* tools then help assign specific locations of all circuit components including standard cells and macro blocks within the circuit's core area. And *Routing* tools will help connect the placed components through metal wires based on specific design rules. Ultimately, the physical layout, often in the format of GDS-II file, will be delivered to the foundry for fabrication. Within each design step, design verification will be performed using *Verification* tools.

Although CAD tools help optimize the circuit performance based on the user-specified constraints, modern CAD tools do not treat the security as one optimization dimension. As a result, fabricated ICs, though satisfying the design specification, may be vulnerable to hardware attacks. Among these security threats, different types of side-channel leakages, including power, EM, timing, light, acoustic, etc., are prevailingly available to circuits dealing with sensitive information. These side-channel leakages can be exploited by an attacker to extract secret information with the help of multiple statistical techniques. We call the whole information leaking exploitation as side-channel analysis (SCA) attacks. To counter these attacks, various countermeasures have been developed recently. Most of these solutions are based on architectural level or circuit level optimization with significant area and power overheads. There lacks CAD tools for circuit security enhancement. In fact, previous work has already proved that CAD tools contribute to side-channel leakages through the current design optimization process [1]. For example, placement tools optimize register locations to minimize clock skews, resulting in synchronous information leakages in the time domain.

Upon this observation, different from existing approaches, we try to mitigate SCA threats by developing new CAD tools with security as one constraint. To demonstrate the feasibility of the proposed CAD for security solutions, in this paper, we take EM for example and developed a placement CAD tool for EM side-channel protection.

EM radiation is derived from current flows within ICs, containing rich information in spatial, temporal and frequency domain, and can be measured in a non-contact way. With the advancement of experimental facilities, all the above natural characteristics of EM radiation have been taken full advantage of by localized EM SCA attacks [2]. Utilizing high-resolution magnetic probes, localized EM SCA attacks are more effective and even nullify traditional countermeasures against power SCA attacks, such as dual-rail logic [3] and threshold implementation [4].

Given the severity of EM side channel leakage, researchers started to investigate the characteristics of EM leakage in the context of side-channel security very recently but these works ignore the impact of CAD tools on EM leakage [5]. In this paper, we first construct an EM leakage model to explore the root-cause of EM leakage in the layout design flow. Specifically, the impact on EM leakage introduced by placement is analyzed and mathematical proofs are provided

978-1-7281-3544-1/19/$31.00 © 2019 IEEE

to demonstrate the feasibility of security-driven placement on improving the EM SCA resilience. With the understanding of the EM leakage causes, we then develop one of CAD for security tools, **CAD4EM-P: CAD for EM Security-Placement**. The tool can help improve the circuit resistance against EM SCA attacks with trivial overheads and can be easily integrated into the modern IC design flow. The core concept of the proposed security-driven placement tool is to navigate data-dependent register reallocation to maximize EM leakage deviation, and thus reduce EM side-channel leakages.

The main contributions of the paper are listed as follows:

- An automatic security-driven placement CAD tool, named **CAD4EM-P**, is developed and evaluated. This tool can be integrated into the modern IC design flow and reduces EM leakage by register reallocation with trivial area and power overheads.
- EM leakage model is constructed to demonstrate that although EM leakage is mainly derived from the on-chip power grid, its time-domain distribution is affected by the placement process.
- Layout-level EM simulations have been performed. Experimental results demonstrate the soundness of the leakage model and the validity of the **CAD4EM-P** tool.

The rest of the paper is organized as follows. Section II presents the background. Section III provides the leakage model of the security-driven placement. Section IV shows the details of the **CAD4EM-P** tool. Section V analyzes the experimental results and a conclusion is drawn in Section VI.

II. Background

A. Performance-Driven Placement

In the back-end of an IC design flow, placement typically consists of three consecutive stages: *global placement*, *legalization* and *detailed placement*, where *global placement* produces a rough placement solution for movable cells, *legalization* then removes cell overlapping by moving cells minimally, and *detailed placement* further improves the legalized placement with respect to a given objective [6].

Most of current placement tools and techniques are performance-driven which perform the optimization under multiple quality objectives, such as wirelength, routability, timing and power. Clock network optimization involving register placement plays an important role in performance-driven placement. To achieve this goal, Cheon et al. propose a power-aware placement method involving activity-based register clustering to reduce the clock power consumption [7]. Lu et al. minimize clock network wirelength by navigating register locations in the quadratic placement [8]. In [9], a modified K-means algorithm is proposed to perform register clustering at the post-global placement step.

The basic concept of these methods is to place registers closer to each other in a cluster, and all registers are placed as close as possible to the clock buffer. Thus the total clock wirelength and clock skew can be reduced significantly. However, these wire delay balancing strategies make side-channel leakage of data-dependent registers occur simultaneously, which will facilitate point-by-point SCA attacks and thus increase the security threat.

B. EM Side Channel Analysis Countermeasures

To prevent and mitigate EM SCA attacks, various countermeasures have been proposed. In traditional EM countermeasures, modification of algorithm, architecture or logic description of cryptographic devices is applied [10]. Recently, several on-chip voltage regulators have been exploited to suppress EM emissions and improve EM SCA resistance. In [11], the authors investigate the security impact of on-chip voltage regulators on EM leakage signature. In [12], Kar et al. integrate a high-frequency inductive voltage regulator (IVR) that acts as an EM emitter to mislead an adversary ($> 100\%$ area overhead). In [13], random fast voltage dithering (RFVD) enabled by an on-package high-frequency IVR is proposed to increase the EM SCA resistance ($+6.6\%$ area, -3.5% power overhead). In [5], a technique named STELLAR is proposed to suppress EM radiation by locally routing the entire cryptographic IP in low-level metal layers and embedding the IP within the Signature Attenuating Hardware ($+22.85\%$ area, $+49\%$ power overhead).

However, most of these countermeasures introduce significant area and power overheads [12]. Meanwhile, to secure ICs against EM SCA attacks, a designer needs at least the backgrounds of both hardware design and side-channel security, which hinders the widespread applications of these approaches. Hence, developing an automatic CAD tool integrated into the current design flow shows a promising prospect for resilient IC designs with a balance among design effort, performance overheads, and security.

III. EM Analysis of Security-driven Placement

In this section, the root-cause of EM leakage in IC back-end design, especially in layout design is investigated. Mathematical proofs are provided to analyze the feasibility of security-driven placement for enhancing EM SCA attack resistance.

A. Root-Cause of EM Leakage in Layout

When designing the IC layout, the step of power planning constructs the power distribution network utilizing a mesh structure. Local grids use the lowest metal layer and global grids use the uppermost metal layers. Then placement builds the cell-level transistor layer on the silicon substrate and signal lines are laid out over multiple metal layers during routing. A typical IC layout topology is shown in Figure 1.

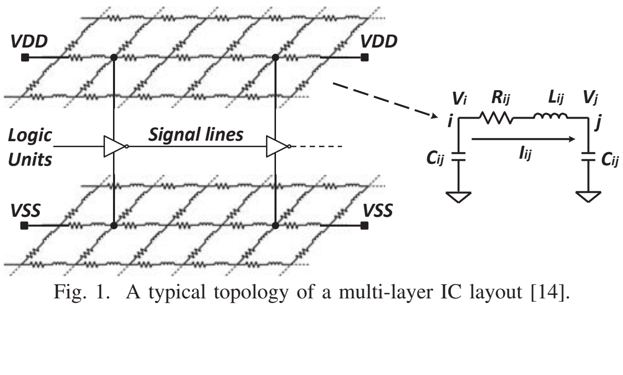

Fig. 1. A typical topology of a multi-layer IC layout [14].

Cells draw current from the local power grids, while external power is supplied to the global grids via input/output (I/O) pads. Hence, due to the switching activities of gates, generated time-varying currents flow within the multi-layer IC emanate EM radiation according to Maxwell's equations. Considering an N-metal layer IC, each metal line is represented as a set of connected segments separated by vias, and each segment can be modeled as a $\pi-$type equivalent circuit [15]. According to Kirchhoff's law, the branch current and node voltage of a segment in the n-th metal layer can be calculated as

$$\begin{aligned} V_i - V_j &= L_{ij}\frac{dI_{ij}}{dt} + R_{ij}I_{ij} \\ I_{ij} + C_{ij}\frac{dV_i}{dt} &= 0 \quad for\ Node\ i \\ I_{ij} - C_{ij}\frac{dV_j}{dt} &= 0 \quad for\ Node\ j \end{aligned} \tag{1}$$

where V_i and V_j are the voltages at i-th node and j-th node, I_{ij} is the current flow from i-th node to j-th node, R_{ij} and L_{ij} are wire resistance and inductance, and C_{ij} is the node capacitance.

Let $\hat{\nu}$ denote the direction of the branch current I_{ij}, the magnetic field emanated by this segment can be computed and one of the solutions for these equations satisfying $R_{ij}^2 = 8L_{ij}/C_{ij}$ is listed:

$$\overrightarrow{H}(\overrightarrow{r},t) = \iint_{l\cdot w} \hat{r} \times \frac{\left[(C_1 + C_2 t)e^{-\frac{R_{ij}}{2L_{ij}}t}\right]\cdot\hat{\nu}}{4\pi w r^2} ds \tag{2}$$

where l and w are the length and width of the metal segment, respectively, r and $\widehat{r}$ are the magnitude and direction of the vector $\overrightarrow{r}$ that is directed from the source point to the observer point. C_1 and C_2 are constants. Note that the shielding effect of the upper layers is negligible since we focus on ICs operating at low frequency.

From Equation 1 and Equation 2, it can be deduced that the dimension-dependent impedance of metal lines has a significant effect on the branch current, and thus the EM radiation. Since power grids often use larger dimension metal layers than signal lines in the layout, larger branch currents will flow through these metal lines and will emanate dominant EM radiation. Therefore, the EM radiation emanated by signal lines is negligible. The distribution of the overall EM radiation in the time domain is affected by signal lines due to the dimension-dependent signal delays, which are partially regulated by placement.

B. Effect of Security-driven Placement on EM Leakage

To analyze the EM SCA resilience introduced by placement, Correlation EM Analysis (CEMA) attack is exploited in this paper. CEMA retrieves the correct key by calculating the Pearson correlation coefficient between EM traces $\boldsymbol{H_{overall}}$ and EM leakage model $\boldsymbol{W}$.

As we mentioned in Section II-A, in traditional performance-driven placement, registers are placed together and are close to the clock buffer to balance the signal delays from the clock to these registers. Transient EM leakage of these registers is thus generated synchronously. In this situation, the total EM radiation is typically decomposed into three components and presented in Equation 3. $\boldsymbol{H_d}$ denotes the data-dependent EM radiation that mostly comes from the dynamic switching of registers. $\boldsymbol{H_{ind}}$ denotes the data-independent EM radiation and $\boldsymbol{H_n}$ is EM noise caused by other parts of metal layers.

$$H_{overall} = H_d + H_{ind} + H_n \tag{3}$$

While in security-driven placement, we try to break the balance of signal delays by register reallocation under the condition of layout constraints. Hence, there is a variation of $\boldsymbol{H_\Delta}$ on the transient data-dependent EM radiation due to the existence of signal deviation Δ starting from the clock source to data-dependent registers. The overall EM radiation considering the effect of placement is then extended as

$$H_{overall} = H_d + H_{ind} + H_n + H_\Delta \tag{4}$$

Since $\boldsymbol{H_{ind}}$, $\boldsymbol{H_n}$ and $\boldsymbol{H_\Delta}$ are orthogonal with $\boldsymbol{H_d}$ and $\boldsymbol{W}$, respectively, the Pearson correlation coefficient between $\boldsymbol{H_{overall}}$ and $\boldsymbol{W}$ can be derived as

$$\begin{aligned} \rho(W, H_{overall}) &= \frac{E(W\cdot H_{overall}) - E(W)\cdot E(H_{overall})}{\sqrt{Var(W)\cdot Var(H_d + H_{ind} + H_n + H_\Delta)}} \\ &= \frac{E(W\cdot H_d) - E(W)\cdot E(H_d)}{\sqrt{Var(W)\cdot Var(H_d)}\sqrt{1+\frac{Var(H_\Delta)}{Var(H_d)}}\sqrt{1+\frac{Var(H_{ind}+H_n)}{Var(H_d+H_\Delta)}}} \\ &= \frac{\rho(W\cdot H_d)}{\sqrt{1+\frac{1}{SNR}}}\cdot\frac{1}{\sqrt{1+\frac{Var(H_\Delta)}{Var(H_d)}}} \end{aligned} \tag{5}$$

where $E(\cdot)$ and $Var(\cdot)$ are functions of calculating mean and variance of a set, respectively. SNR denotes the signal-to-noise ratio between $\boldsymbol{H_{ind}} + \boldsymbol{H_n}$ and $\boldsymbol{H_d} + \boldsymbol{H_\Delta}$ in the attack. Therefore, the correlation coefficient can be reduced by register reallocation and inversely proportional to $Var(H_\Delta)$.

IV. CAD for EM Security Tools

Based on the above discussion, the EM SCA resistance enhancement problem can be reduced to a security-driven placement problem. **CAD4EM-P** is then proposed to solve this problem.

A. Framework of CAD4EM-P

Given an initial legalized placement after Clock Tree Synthesis (CTS), **CAD4EM-P** will optimize the placement to maximize leakage deviation through steps in Algorithm 1.

Algorithm 1 describes the detailed framework of the proposed **CAD4EM-P** tool. We first construct a graph $\boldsymbol{G(V,E)}$ to represent the given initial placement, with vertex set $\boldsymbol{V = \{v_1, v_2, ..., v_{m+n}\}}$ denoting locations of fixed-positioned clock tree $\boldsymbol{K = \{k_1, k_2, ..., k_m\}}$ and movable data-dependent registers $\boldsymbol{F = \{f_1, f_2, ..., f_n\}}$ and $\boldsymbol{E = \{e_1, e_2, ..., e_p\}}$ indicating the signal connections among these cells (Line 1).

Lines 2-4 describe the *Reallocation Boundary Construction* process. For any register in set $\boldsymbol{F}$, its location is determined by the given clock latency constraint. That is, register relocation must follow the rule that its routing clock signal delay does not

Algorithm 1 Security-Driven Placement

```
Input:   Placement design, timing and area constraints
Output:  New Placement
 1: Constructing Placement Graph $\boldsymbol{G(V,E)}$
    //Reallocation Boundary Construction
 2: $s_0 = (x_0, y_0) \leftarrow \boldsymbol{S_{clk}}, \boldsymbol{S_{reg}}$
 3: $l_{max} \leftarrow r_w, c_w, R_d, C_l, T_{CL}$
 4: Boundary: Manhattan Ring $\boldsymbol{C_{bd}} \leftarrow l_{max}, s_0$
    //Data-dependent Register Reallocation
 5: repeat
 6:   for all $f_i \in \boldsymbol{F}$ do
 7:     $\boldsymbol{R_{rand}} = \{R_{ri}\} \leftarrow$ Randomize location for $f_i$
 8:     if $\boldsymbol{R_{rand}} \subset \boldsymbol{C_{bd}}$ and $\boldsymbol{R_{rand}} \cap \boldsymbol{R_{clk}} = \emptyset$ then
 9:       $\boldsymbol{R_{feasible}} \leftarrow \boldsymbol{R_{rand}}$
10:       $\boldsymbol{S'_{reg}} \leftarrow \boldsymbol{S_{reg}}$
11:     end if
12:   end for
13:   for all $s'_i \in \boldsymbol{S'_{reg}}$ do
14:     $\boldsymbol{L_{path}} = \{L(s_0, s'_i)\} \leftarrow d_m(s_0, s'_i)$
15:     $\boldsymbol{D_{path}} = \{T_{Delay,i}\} \leftarrow \boldsymbol{L_{path}}, R_d, C_l, r_w, c_w$
16:   end for
17: until Maximum $Var(\boldsymbol{D_{path}})$
18: Updating Placement Graph $\boldsymbol{G(V,E)}$
```

exceed the prescribed maximum clock latency T_{CL}. Therefore, the boundary for register reallocation is built based on the maximum routing length l_{max} which can be extracted from the given timing constraint.

We model the data-dependent clock buffer and clock signal wire as an RC connection [16], [17]. The wire delays from this clock buffer to related registers can be computed using the Elmore delay model. To meet the clock latency constraint, the maximum routing length l_{max} can be obtained as:

$$l_{max} = \frac{\sqrt{c_w^2 R_d^2 + r_w^2 C_l^2 + 2 r_w c_w T_{CL}} - c_w R_d - r_w C_l}{r_w c_w} \tag{6}$$

where r_w and c_w are the unit resistance and capacitance of the wire, respectively, R_d is the driver resistance of the buffer, and C_l is the load capacitance. We then construct the boundary using Manhattan ring [8] to restrict the following register reallocation. Manhattan ring $\boldsymbol{C_{bd}}$ is a $45°$-tilted square with the same Manhattan distance l_{max}, from the center on the clock buffer pin s_0 with the coordinate (x_0, y_0) to any point on it. Any reallocation of these data-dependent registers outside this boundary is prohibited. Note that the boundary is directly affected by the drive strength of the clock buffer due to the nonlinear relation between R_d and l_{max}.

Lines 5-17 describe the *Data-dependent Register Reallocation* process. For all data-dependent registers $\boldsymbol{F}$, we randomize their location regions $\boldsymbol{R_{rand}} = \{R_{r1}, R_{r2}, ..., R_{rn}\}$ that consist of their locations $\boldsymbol{V}$ and sizes in the prescribed boundary, satisfying the area constraint to avoid any overlaps among $\boldsymbol{R_{rand}}$ and fixed-positioned clock tree location regions $\boldsymbol{R_{clk}}$. Through iterations, the feasible register location regions $\boldsymbol{R_{feasible}}$ and corresponding pins $\boldsymbol{S'_{reg}}$ are obtained, as shown in Lines 6-12.

Meanwhile, for any register pin s'_i in set $\boldsymbol{S'_{reg}}$, we calculate each path length $L(s_0, s'_i)$ from s_0 to s'_i by Manhattan distance. Moreover, the related path delay set $\boldsymbol{D_{path}} = \{T_{Delay,i}\}$ is obtained based on the path length set $\boldsymbol{L_{path}}$ using the Elmore delay (see Lines 13-16). To attain optimal solution of the security-driven placement problem, multiple round iterations are performed until the maximum $Var(\boldsymbol{D_{path}})$ is met, an indication that a linear relation exists between $\boldsymbol{H_{\Delta}}$ and $\boldsymbol{D_{path}}$. Placement graph $\boldsymbol{G(V,E)}$ is updated to acquire a new placement with optimum EM SCA resistance.

*B. Integrating **CAD4EM-P** to Existing Design Flow*

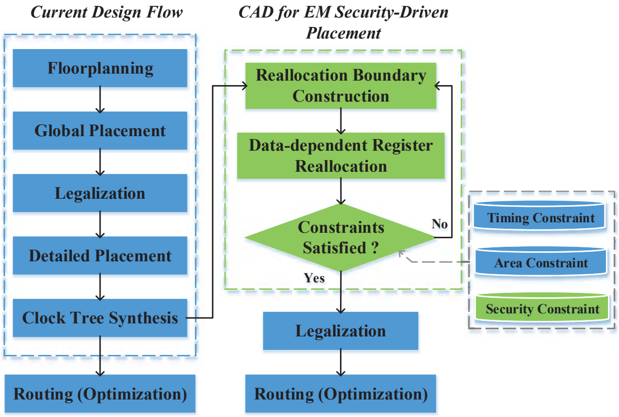

Fig. 2. CAD4EM-P integration to the current design flow.

As shown in Figure 2, **CAD4EM-P** can be easily integrated into current IC design flow and perform security optimization after CTS. This tool parses design files, i.e., *design.place*, *design.lef* and *design.def*, to obtain original locations, statuses, connections of clock tree and user-defined registers. Using the above information, a placement graph $\boldsymbol{G(V,E)}$ is built. Meanwhile, **CAD4EM-P** requires timing constraint file *design.sdc* and library database to construct a reallocation boundary. The timing constraint file contains timing information about clock latency, and the library database includes parasitic information of cells and wires. Then this tool randomizes locations of data-dependent registers in specified round iterations, generates a list that consists of feasible register locations. Delay computation is also performed and the obtained $Var(\boldsymbol{D_{path}})$ set serves as a security metric for location list ranking. The final placement file is obtained by replacing the locations of each register by their optimum counterparts. Both clock buffers and data-dependent registers are fix-positioned through status editing.

Inevitably, there will be several overlaps between fix-positioned cells and other irrelevant components after the security-driven placement. Thus, the new placement file will be re-imported to the layout design tool and legalization is performed again to remove these introduced cell overlaps. Finally, the layout with optimum EM SCA resistance is generated by routing with optimization processes in the existing design flow.

V. Experimental Results

In this section, we will validate the developed EM leakage model and the efficacy of proposed **CAD4EM-P** tool, utilizing layout-level EM simulation methodology on AES designs[1].

A. Simulation Setup

For an AES design, one of the optimal attack targets is typically the moment when the AES circuit executes SubBytes (S-Box) operations. Since CEMA attacks reveal the secret key through byte-by-byte analysis, the dynamic switching of other parts such as remaining S-Boxes can be treated as intrinsic noises. In our simulation, two simplified versions of AES circuits that encrypt one-byte plaintext are used to accelerate the simulation process [18]. These circuits compose of SubBytes, ShiftRows, and AddRoundKey and form the last-round datapath of AES encryption. This irrelevant datapath removing aims to reduce the noise level in EM SCA when recovering a particular key-byte. Hence, successful protection in this situation is also adequate for normal AES implementations.

The first circuit contains S-Box implemented with Galois Field (GF) algorithm, where complicated computation leads to high area overhead, denoted as AES-GF. The second circuit exploits look-up table (LUT) based S-Box, in which data fetching from vast of memory results in high power consumption, denoted as AES-LUT. Their RTL descriptions are synthesized using SMIC 180nm logic technology in Synopsys Design Compiler, and then placed and routed using Cadence SOC Encounter. The physical layout consists of four metal layers, where M4 and M3 are used for global power routing and M1 is used for local power routing. Signal lines lay over all metal layers. The clock frequency and the supply voltage of this circuit are 20 MHz and 1.8 V, respectively. Compared with the non-protected circuits, the only difference of the protected designs is that **CAD4EM-P** is applied to help generate the layout (see Figure 2). The tool requires 19 minutes to execute 500 round iterations and generates an optimum placement.

Considering the requirement for evaluating the EM leakage during IC layout design flow, the layout-level simulation method in [19] is utilized. This type of method has been validated in [20], where good agreement between the simulated EM radiation and measured data exists.

B. Validation of EM Leakage Root-Cause in Layout

To validate our theoretical analysis, we investigate the contributions of signal lines and power grids in terms of EM intensity and CEMA attacks. We set the probe height $D = 30\mu\text{m}$ to mimic the actual environment of localized EM SCA attacks [3], [4].

For each individual metal layer, average magnetic field amplitudes from signal lines and power grids during 256 encryptions are listed in Table I. As shown in the table, the intensity of the EM radiation from power grids is significantly larger than that from signal lines by a factor of at least 10×.

TABLE I
Average magnetic field amplitudes from signal lines vs power grids in each metal layer

Avg. H-Field Amplitude	**Metal1**	**Metal2**	**Metal3**	**Metal4**
Fr. Signal Lines $(\mathrm{A/m})$	0.0200	0.0017	0.1674	0.0262
Fr. Power Grids $(\mathrm{A/m})$	0.6139	0.0163	1.7875	2.3355
Ratio (Power / Signal)	30.70×	9.59×	10.68×	89.14×

Moreover, we construct EM information maps to compute the contribution of signal lines in the context of side-channel security according to Equation 7. CEMA attacks are performed on each point of the circuit's surface, and the maximum correlation coefficient is used to indicate the information leakage of this point. Simulation results show that only 2.91% of information leakage comes from signal lines.

$$Contribution = Avg.\ \frac{Leakage\ Matrix \mid signal}{Leakage\ Matrix \mid power+signal} \quad (7)$$

Based on these results, it is concluded that the amount of EM leakage mostly comes from power grids in the layout whereas the leakage from signal lines is negligible.

C. Efficacy of **CAD4EM-P** against EM SCA Attacks

Figure 3 presents the information leakage maps of AES-GF and AES-LUT by localized CEMA attacks. The color bar is used to quantify the degree of the EM information leakage, in which the topmost color denotes that this point leaks maximum EM information exploited by an attacker. Evidently, the EM information leakage is significantly reduced compared with non-protected circuits, with the maximum correlations decreasing by 54.41% and 27.84%, respectively.

Meanwhile, the CEMA results for EM information leakage points with maximum correlation are shown in Figure 4, where red and green traces denote the correlation of the correct key of the non-protected and protected circuits, respectively. Blue traces represent the correlation of the incorrect keys. The correlation coefficients of the correct key decrease and submerge in those of incorrect keys, showing that all points of circuits' surface are successful protected. It is validated that the proposed tool **CAD4EM-P** can effectively improve the circuit's resistance against EM SCA attacks.

Table II lists the overheads of **CAD4EM-P**. Compared to non-protected circuits, zero-area overhead is introduced since the *Data-dependent Register Reallocation* process is confined to the area of initial placement. Moreover, the average power consumption of the protected designs slightly increases by 1.48% and 2.43%. The primary reason is that the increased total wirelength causes higher power consumption.

VI. Conclusion

In this paper, we propose a CAD for security tool **CAD4EM-P** to consider security attributes within the modern IC design flow against EM SCA attacks. The key concept is the observation that the amount of EM leakage mostly

[1] Please note that the developed tool can be applied to all circuit designs for EM side channel protection.

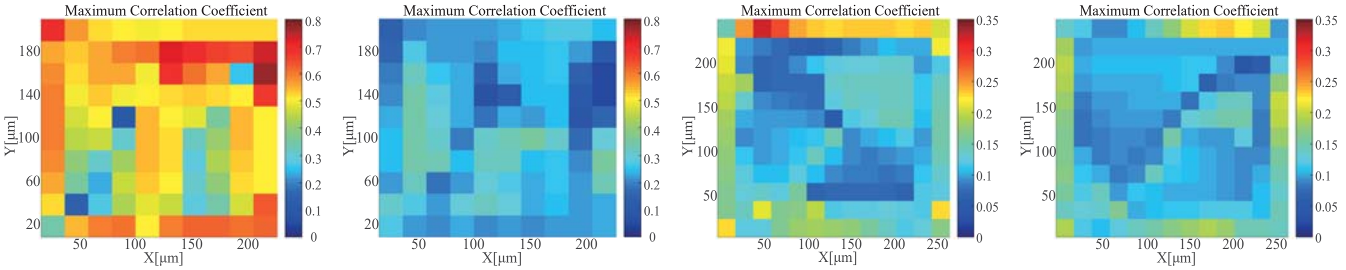

Fig. 3. EM information leakage maps of (a) non-prot. AES-GF, (b) prot. AES-GF, (c) non-prot. AES-LUT, (d) prot. AES-LUT.

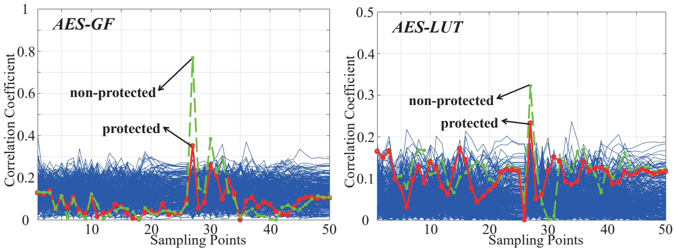

Fig. 4. CEMA results for EM leakage hot spots of (a) AES-GF (b) AES-LUT.

TABLE II
BALANCE OF SECURITY AND PERFORMANCE OVERHEADS

Exper.	Max. Correlation	Tot. Area(μm^2)	Avg. Power(mW)
Non-prot. I	0.7684	50575	1.5359
Prot. I *	0.3503(**-54.41%**)	50575(**+0%**)	1.5586(**+1.48%**)
Non-prot. II	0.3226	65950	0.4936
Prot. II*	0.2328(**-27.84%**)	65950(**+0%**)	0.5056(**+2.43%**)

* I denotes AES-GF and II denotes AES-LUT.

comes from power grids while its temporal distribution is regulated by placement. **CAD4EM-P** helps optimize the initial placement to maximize EM leakage deviation by solving the security-driven placement problem. Utilizing the EM simulation method at layout-level, experiment results show that **CAD4EM-P** can protect simplified versions of AES circuits against EM SCA attacks with the maximum correlation reduced by 54.41% and 27.84%, respectively, with trivial performance overheads. In our future work, we will investigate and develop more CAD for security tools for circuit protection in an automatic way.

ACKNOWLEDGMENT

Dr. Jiaji He is supported by the China Postdoctoral Science Foundation under Grant 2019TQ0167.

REFERENCES

[1] K. Tiri and I. Verbauwhede, “A vlsi design flow for secure side-channel attack resistant ics,” in *Design, Automation and Test in Europe*. IEEE, 2005, pp. 58–63.

[2] J. Heyszl, D. Merli, B. Heinz, F. De Santis, and G. Sigl, “Strengths and limitations of high-resolution electromagnetic field measurements for side-channel analysis,” in *International Conference on Smart Card Research and Advanced Applications*. Springer, 2012, pp. 248–262.

[3] V. Immler, R. Specht, and F. Unterstein, “Your rails cannot hide from localized em: how dual-rail logic fails on fpgas,” in *International Conference on Cryptographic Hardware and Embedded Systems*. Springer, 2017, pp. 403–424.

[4] R. Specht, V. Immler, F. Unterstein, J. Heyszl, and G. Sig, “Dividing the threshold: Multi-probe localized em analysis on threshold implementations,” in *2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. IEEE, 2018, pp. 33–40.

[5] 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. 2019 IEEE Int. Symp. Hardw. Oriented Security Trust*, 2019.

[6] A. B. Kahng, J. Lienig, I. L. Markov, and J. Hu, *VLSI physical design: from graph partitioning to timing closure*. Springer Science & Business Media, 2011.

[7] Y. Cheon, P.-H. Ho, A. B. Kahng, S. Reda, and Q. Wang, “Power-aware placement,” in *Proceedings. 42nd Design Automation Conference, 2005.* IEEE, 2005, pp. 795–800.

[8] Y. Lu, C. Sze, X. Hong, Q. Zhou, Y. Cai, L. Huang, and J. Hu, “Navigating registers in placement for clock network minimization,” in *Proceedings. 42nd Design Automation Conference, 2005.* IEEE, 2005, pp. 176–181.

[9] G. Wu, Y. Xu, D. Wu, M. Ragupathy, Y.-y. Mo, and C. Chu, “Flip-flop clustering by weighted k-means algorithm,” in *Proceedings of the 53rd Annual Design Automation Conference*. ACM, 2016, p. 82.

[10] A. A. Pammu, K.-S. Chong, and B.-H. Gwee, “Highly secured arithmetic hiding based s-box on aes-128 implementation,” in *2016 International Symposium on Integrated Circuits (ISIC)*. IEEE, 2016, pp. 1–4.

[11] A. W. Khan, T. Wanchoo, G. Mumcu, and S. Köse, “Implications of distributed on-chip power delivery on em side-channel attacks,” in *2017 IEEE International Conference on Computer Design (ICCD)*. IEEE, 2017, pp. 329–336.

[12] M. Kar, A. Singh, S. Mathew, S. Ghosh, A. Rajan, V. De, R. Beyah, and S. Mukhopadhyay, “Blindsight: Blinding em side-channel leakage using built-in fully integrated inductive voltage regulator,” *arXiv preprint arXiv:1802.09096*, 2018.

[13] A. Singh, M. Kar, S. K. Mathew, A. Rajan, V. De, and S. Mukhopadhyay, “Improved power/em side-channel attack resistance of 128-bit aes engines with random fast voltage dithering,” *IEEE Journal of Solid-State Circuits*, vol. 54, no. 2, pp. 569–583, 2019.

[14] K. Gala, V. Zolotov, R. Panda, B. Young, J. Wang, and D. Blaauw, “On-chip inductance modeling and analysis,” in *Proceedings of the 37th Annual Design Automation Conference*. ACM, 2000, pp. 63–68.

[15] J. Choi, M. Swaminathan, N. Do, and R. Master, “Modeling of power supply noise in large chips using the circuit-based finite-difference time-domain method,” *IEEE transactions on electromagnetic compatibility*, vol. 47, no. 3, pp. 424–439, 2005.

[16] J. Lu, W.-K. Chow, and C.-W. Sham, “Fast power-and slew-aware gated clock tree synthesis,” *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 20, no. 11, pp. 2094–2103, 2011.

[17] Z.-W. Chen and J.-T. Yan, “Routability-driven flip-flop merging process for clock power reduction,” in *2010 IEEE International Conference on Computer Design*. IEEE, 2010, pp. 203–208.

[18] X. Wang, W. Yueh, D. B. Roy, S. Narasimhan, Y. Zheng, S. Mukhopadhyay, D. Mukhopadhyay, and S. Bhunia, “Role of power grid in side channel attack and power-grid-aware secure design,” in *Proceedings of the 50th Annual Design Automation Conference*. ACM, 2013, p. 78.

[19] A. Kumar, C. Scarborough, A. Yilmaz, and M. Orshansky, “Efficient simulation of em side-channel attack resilience,” in *2017 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, Nov 2017, pp. 123–130.

[20] V. Lomné, P. Maurine, L. Torres, T. Ordas, M. Lisart, and J. Toublanc, “Modeling time domain magnetic emissions of ics,” in *International Workshop on Power and Timing Modeling, Optimization and Simulation*. Springer, 2010, pp. 238–249.