Security-Driven Placement and Routing Tools for Electromagnetic Side-Channel Protection

Haocheng Ma, Jiaji He, Yanjiang Liu, Leibo Liu, *Senior Member, IEEE*, Yiqiang Zhao, *Member, IEEE*, and Yier Jin, *Senior Member, IEEE*

***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 overheads and impose high requirements of side-channel security backgrounds to integrated circuit (IC) designers. In this article, we propose an automatic computer-aided design (CAD) tool that can be utilized to enhance the circuit resistance against electromagnetic (EM) SCA attacks. This new tool will guide security-driven placement and routing processes 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 the layout level and mathematically demonstrate the feasibility of security-driven placement and routing 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 register reallocation and wire length adjustments. Simulation results on cryptographic circuits prove the effectiveness of both the constructed EM leakage model and the EM model-based CAD tool for EM side-channel security.**

***Index Terms*—Computer-aided design (CAD) for security, electromagnetic (EM) leakage, placement, routing, side-channel attack.**

I. Introduction

COMPUTER-AIDED design (CAD) tools play important roles in modern integrated circuit (IC) 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 register transfer level (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. *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 the 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 user-specified constraints, modern CAD tools do not treat security as one optimization dimension. As a result, fabricated ICs, though satisfying the design specification, may be vulnerable to various attacks. Among these security threats, different types of side-channel leakages, including power, electromagnetic (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 statistical and data analysis 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 optimizations with significant area and power overheads. There lacks CAD tools for circuit security enhancement. In fact, previous work has already proved that CAD tools involved at different design stages affect side-channel vulnerabilities in direct or indirect ways [1]. For example, synthesis tools like high-level synthesis lead to different levels of side-channel leakages during memory-based architectural optimizations [2]. Placement tools optimize register locations to minimize clock skews, resulting in synchronous information leakages in the time domain [3].

Upon this observation, different from existing approaches, we try to mitigate SCA threats by developing new CAD tools with security as one constraint. Note that the goal for security enhancement can be realized at different stages of the CAD flow. To demonstrate the feasibility of the proposed CAD for security solutions, in this article, we take EM for example, and develop placement and routing 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 noncontact way. With the advancement of experimental facilities, all the above natural characteristics of EM radiation have been exploited by localized EM SCA attacks [4]. Utilizing high-resolution magnetic probes, localized EM SCA attacks

Manuscript received March 30, 2020; revised July 9, 2020; accepted September 6, 2020. Date of publication September 21, 2020; date of current version May 20, 2021. The work of Jiaji He was supported by the China Postdoctoral Science Foundation under Grant 2019TQ0167. This article was recommended by Associate Editor W. Hu. *(Corresponding author: Jiaji He.)*

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

Jiaji He and Leibo Liu are with the Institute of Microelectronics, Tsinghua University, Beijing 100084, China (e-mail: jiaji_he@mail.tsinghua.edu.cn; liulb@tsinghua.edu.cn).

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

Digital Object Identifier 10.1109/TCAD.2020.3024938

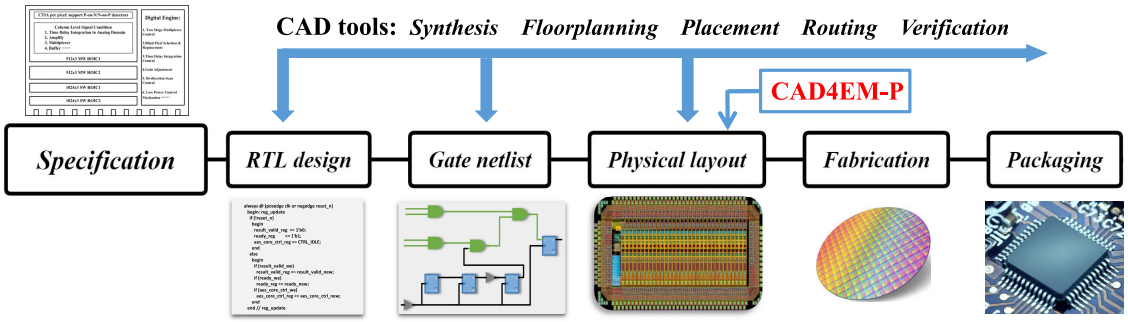


Fig. 1. Overview of the IC design flow and the integration of the proposed CAD4EM-P tools.

are more effective and even nullify traditional countermeasures against power SCA attacks, such as dual-rail logic [5] and threshold implementation [6].

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 [7]. In this article, 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 and routing is analyzed and mathematical proofs are provided to demonstrate the feasibility of security-driven placement and routing on improving the EM SCA resilience. With the understanding of EM leakage causes, we then develop a CAD for security tool, *CAD4EM-P—CAD for EM Security-Placement:* the tool can help improve the circuit's resistance against EM SCA attacks with reasonable overheads and can be easily integrated into the modern IC design flow. Fig. 1 shows a typical IC design flow and the stage where CAD4EM-P will be applied. The proposed tool will execute two successive optimizations to increase the inner deviation of EM side-channel leakage: 1) security-driven placement navigates data-dependent register reallocation and 2) security-driven routing guides relevant wire length adjustments. In this way, chaotic EM distribution leads to reduced information relevance.

The main contributions of this article are listed as follows.

1) An automatic security-driven placement and routing CAD tool, named CAD4EM-P, is developed and evaluated. This tool can be integrated into the modern IC design flow. Through register reallocation and wire length adjustments, the data dependency of EM leakage is reduced under reasonable area and power overheads.
2) 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 and routing processes.
3) Layout-level EM simulations have been performed, where experimental results demonstrate the soundness of the leakage model and the validity of the CAD4EM-P tool.

The remainder of this article is organized as follows. Section II presents the background. Section III provides the leakage model of the security-driven placement and routing. Section IV shows the details of the CAD4EM-P tool and layout-level EM simulation flow. Section V analyzes the experimental results on small-scale circuits, which are protected by security-driven placement only. Then Section VI validates the effectiveness of both security-driven placement and routing on medium-scale circuits. The conclusion is drawn in Section VII.

II. Background

A. Performance-Driven Placement and Routing

In the back-end of an IC design flow, placement typically consists of three consecutive stages: 1) *global placement*; 2) *legalization*; and 3) *detailed placement*, where *global placement* produces a rough placement solution for movable cells, then *legalization* removes cell overlapping by moving cells minimally, and *detailed placement* further improves the legalized placement with respect to a given objective [8]. Similarly, routing is typically composed of two stages: *global routing* followed by *detailed routing*, where *global routing* first creates a coarse routing solution for each net, then *detailed routing* determines the exact routes of all nets [9].

Most of the current placement and routing 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.* [10] proposed a power-aware placement method involving activity-based register clustering to reduce the clock power consumption. Lu *et al.* [11] minimized clock network wirelength by navigating register locations in the quadratic placement. In [12], 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 (see Fig. 2). Thus, the clock skew can be reduced significantly. Furthermore, based on the fact that wire delays depend on the width and length of wires, performance-driven routing, e.g., wire sizing [13]–[15] and wire snaking [16]–[19], can help achieve the zero-skew goal. 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 lead to side-channel security vulnerabilities.

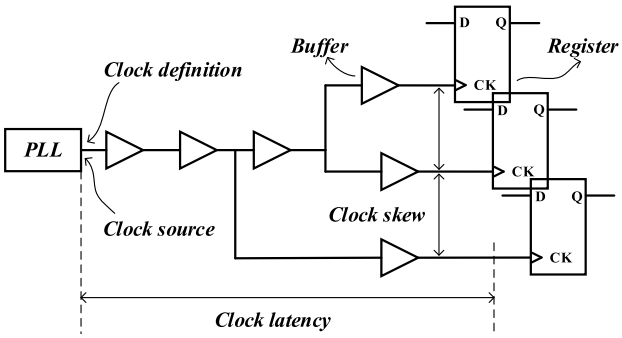


Fig. 2. Clock network and clock skew.

B. EM Side Channel Analysis Attacks

Since Quisquater and Samyde [20] extended the concept of SCA into the EM side-channel domain, large numbers of publications have proven that EM SCA is an enormous threat to various cryptographic algorithms (e.g., AES, DES, and RSA) implemented on different types of electronic devices containing ASIC, FPGA, processor, and smart cards. Considering EM trace collection, the measurement equipment and the distance to die surface are two crucial parameters determining the efficacy of EM SCA attacks. Heyszl *et al.* [4] position the magnetic probe with a diameter 150 μm at a close distance 50 μm to the die surface. This attack, called localized EM attack, shows an improved signal-to-noise ratio (SNR) and spatial resolution compared to power attacks. Also, they observe that the EM leakage is related to registers that are driven by the active clock edges. Further, Immler *et al.* [5] and Specht *et al.* [6] demonstrated that localized EM attack can effectively extract local characteristics of placement and routing, such that power-resistant countermeasures containing dual-rail logic and threshold implementations fail in the EM side channel protection.

C. EM Side Channel Analysis Countermeasures

To prevent and mitigate EM SCA attacks, various countermeasures have been proposed. In traditional EM countermeasures, modifications of algorithm, architecture, or logic description of cryptographic devices are applied [21]. In [1], the secure logic like the wave dynamic differential logic (WDDL) is implemented for energy balance. The area and power overheads increase by 3.4× and 5.9×, respectively. In [22], the leaking electrical paths are allocated randomly to prevent EM attacks, with an area overhead of 3.5×. Recently, several on-chip voltage regulators have been exploited to suppress EM emissions and improve EM SCA resistance. Khan *et al.* [23] investigated the security impact of on-chip voltage regulators on EM leakage signature. Kar *et al.* [24] integrated a high-frequency inductive voltage regulator (IVR) that acts as an EM emitter to mislead an adversary, while the area overhead is greater than 100%. In [25], random fast voltage dithering (RFVD) enabled by an on-package high-frequency IVR is proposed to increase the EM SCA resistance. The protection increases the area overhead by 6.6% with negligible power overhead. In [7], 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. However, the area and power overheads increase by 22.85% and 49%, respectively.

Thus it can be seen that most of these countermeasures introduce significant area and power overheads [24]. Further, these countermeasures often require designers to have sufficient backgrounds on both hardware design and side-channel security, which complicates the effect in adopting these techniques for circuit protection. Although some EDA-friendly solutions are proposed, there lack of optimizations on EDA tools themselves for side-channel security enhancement. As reported in [2], [26], and [27], EDA tools themselves will contribute to the side-channel leakage during current design optimizations. Based on the finding that placement and routing processes will try to optimize power, area, and timing metrics in sacrificing security, we develop the CAD4EM-P that performs security-driven placement and routing to enhance the EM side-channel protection, with a balance among design effort, performance overheads, and security. Due to the generic nature, this tool can also be combined with the existing countermeasures for further higher security improvement.

D. Preprocessing-Based EM Side Channel Analysis

In practice, a skilled attacker will apply certain preprocessing methods on collected traces, which improves the attack efficiency against hiding-based countermeasures. These methods can be separated into two categories in general. The first category aims to align the EM traces in the time domain, such as static alignment (SA) and elastic alignment (EA). SA is proposed by Mangard *et al.* [28]. It first finds reference samples (e.g., rising edge) in collected side-channel traces and then matches the same references by shifting other traces. EA is based on dynamic time warping (DTW), which is a well-established algorithm for time-series matching [29]. This method matches parts of several traces at different offsets and performs nonlinear resampling of the traces.

The second category aims to transform side-channel traces from the time domain to other domains, such as fast Fourier transform (FFT) and principal component analysis (PCA). Based on the fact that a shift in the time domain only slightly alters the amplitude spectrum in the frequency domain, Mateos and Gebotys [30] carry out correlation EM analysis (CEMA) on the processed traces using FFT. PCA utilizes an orthogonal transformation to convert initial variables to a new coordinate space where variables are linearly uncorrelated [31]. In general, the first principal component with the largest variance contains the most important information. In this way, the influence of misalignment in side-channel traces will be removed. In this article, we will validate whether our proposed tool can withstand the above preprocessing-based attacks.

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.

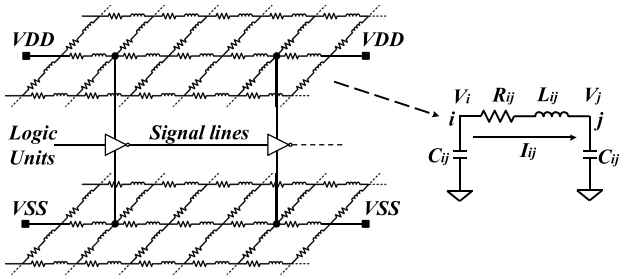


Fig. 3. Typical topology of a multilayer IC layout [32].

Mathematical proofs are provided to analyze the feasibility of security-driven placement and routing 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 Fig. 3.

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 switching activities of gates, generated time-varying currents flow within the multilayer 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 [33]. According to the Kirchhoff's law, branch current and node voltage of a segment in the nth metal layer can be calculated as

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

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

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

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

where l and w are the length and width of the metal segment, respectively, r and $\hat{r}$ 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 (1) and (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 wires 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 and Routing on EM Leakage

To analyze the EM SCA resilience introduced by placement and routing processes, CEMA attack is exploited in this article. CEMA retrieves the correct key by calculating the Pearson correlation coefficient between EM traces H_{overall} and EM leakage model W.

As mentioned in Section II-A, in traditional performance-driven placement, registers are placed together and are close to clock buffers to balance 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 (3). H_d denotes the data-dependent EM radiation that mostly comes from the dynamic switching of registers, H_{ind} denotes the data-independent EM radiation and H_n is EM noise caused by other parts of metal layers

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

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 H_Δ 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

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

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

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

where $E(\cdot)$ and $\text{Var}(\cdot)$ are functions of calculating mean and variance of a set, respectively. SNR denotes the SNR between $H_{\text{ind}} + H_n$ and $H_d + H_\Delta$ in the attack. The recovered key with the maximum Person correlation coefficient

$\rho_{\max} = \max(\rho(W, H_{\text{overall}}))$ indicates the most possible correct key. The lower maximum correlation $\rho_{\max}$ signifies that the cryptographic circuit has more EM side-channel robustness. This means that the adversary requires more EM traces to perform successful EM SCA attacks. Here, we denote the minimum traces required to disclosure the correct key as N_{MTD}. The values of N_{MTD} can be approximately estimated by the $\rho_{\max}$, according to the empirical model reported in [28]

$$N_{\text{MTD}} = 3 + 8\frac{z_{1-\alpha}^2}{ln^2\frac{1+\rho_{\max}}{1-\rho_{\max}}} \tag{6}$$

where $z_{1-\alpha}$ is the quantile of random variables $X \sim N(0, 1)$, and its value leads to the probability $P(X \leq z_{1-\alpha}) = \alpha$. The N_{MTD} along with $\rho_{\max}$ are utilized to evaluate the EM side-channel security of ICs throughout this article.

Taking the correlation coefficient as an example, this security metric can be reduced by register reallocation and inversely proportional to $\text{Var}(H_\Delta)$. Moreover, the relation between H_Δ and Δ can be assumed as linear during a short period [34]. This means that the maximum value of Δ, denoted as $\Delta_{\max}$, is a critical parameter for discretizing the data-dependent EM radiation. By observing that register reallocation subjects to the size of the layout, we can further enhance the EM SCA resilience by security-driven routing. Within the limited core area, we attempt to increase the $\Delta_{\max}$ by wire length adjustments under all constraints. The increased $\Delta_{\max}$ will result in an incremental H_Δ, and thus reduce the correlation coefficient as described in (5).

IV. CAD for EM Security Tools

Based on the above discussion, the EM SCA resistance enhancement problem can be reduced to security-driven placement and routing problems. CAD4EM-P is then proposed to solve these problems. The entire workflow of this tool can be divided into two stages: 1) the security-driven placement involving register reallocation and 2) the security-driven routing involving wire length adjustments.

A. Framework of CAD4EM-P: Security-Driven Placement

Given an initial legalized placement after clock tree synthesis (CTS), CAD4EM-P will optimize the placement to maximize leakage deviation following steps in Algorithm 1.

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

Lines 2–4 describe the *reallocation boundary construction* process. For any register in set 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 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.

Algorithm 1 Security-Driven Placement

Input: Placement design, timing and area constraints
Output: New placement

1: Construct placement graph $G(V, E)$
//Reallocation Boundary Construction
2: $s_0 = (x_0, y_0) \leftarrow S_{clk}$, S_{reg}
3: $l_{\max} \leftarrow r_w$, c_w, R_d, C_l, T_{CL}
4: Boundary: Manhattan ring $C_{bd} \leftarrow l_{\max}$, s_0
//Data-dependent Register Reallocation
5: **repeat**
6: **for all** $f_i \in F$ **do**
7: $R_{rand} = \{R_{ri}\} \leftarrow$ randomize location for f_i
8: **if** $R_{rand} \subset C_{bd}$ *and* $R_{rand} \cap R_{clk} = \emptyset$ **then**
9: $R_{feasible} \leftarrow R_{rand}$
10: $S_{reg}^{'} \leftarrow S_{reg}$
11: **end if**
12: **end for**
13: **for all** $s_i^{'} \in S_{reg}^{'}$ **do**
14: $L_{path} = \{L(s_0, s_i^{'})\} \leftarrow d_m(s_0, s_i^{'})$
15: $D_{path} = \{T_{Delay,i}\} \leftarrow L_{path}$, R_d, C_l, r_w, c_w
16: **end for**
17: **until** *Maximum Var*(D_{path})
18: Updating placement graph $G(V, E)$

We model the data-dependent clock buffer and clock signal wire as an RC connection [35], [36]. The wire delays from this clock buffer to related registers can be computed using the Elmore delay model. To meet the clock latency constraints, the maximum routing length $l_{\max}$ can be obtained as

$$l_{\max} = \frac{\sqrt{c_w^2 R_d^2 + r_w^2 C_l^2 + 2 r_w c_w T_{\text{CL}}} - c_w R_d - r_w C_l}{r_w c_w} \tag{7}$$

where r_w and c_w are unit resistance and capacitance of the wire, respectively, R_d is driver resistance of the buffer, and C_l is load capacitance. We then construct the boundary using Manhattan ring [11] to restrict the following register reallocation. Manhattan ring 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. This center is one of clock buffer pins S_{clk} which directly drives pins S_{reg} of data-dependent registers. 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 F, we randomize their location regions $R_{\text{rand}} = \{R_{r1}, R_{r2}, \ldots, R_{rn}\}$ that consist of their locations V and sizes in the prescribed boundary, satisfying the area constraint to avoid any overlaps among R_{rand} and fixed-positioned clock tree location regions R_{clk}. Through iterations, the feasible register location regions R_{feasible} and corresponding pins S'_{reg} are obtained, as shown in lines 6–12.

Algorithm 2 Security-Driven Routing

Input: Routed design, timing and area constraints
Output: Optimum physical layout
1: **if** $A_{CORE} < C_{bd}$ **then**
2: Extract routing network R_{Net}
3: Data-independent routing network $R_{INet} \leftarrow \varnothing$
4: **for all** wire $w_{ire} \in R_{Net}$ **do**
5: **if** w_{ire} does not belong to data-dependent path **then**
6: $R_{INet} = R_{INet} \cup w_{ire}$
7: **end if**
8: **end for**
9: Construct the feasible routing region $\leftarrow A_{DR}$
10: **end if**
11: $R_{DNet} = R_{Net} - R_{INet}$
12: **repeat**
13: **for all** $w_{ire} \in R_{DNet}$ **do**
14: Wire snaking $\leftarrow \{D_{\max}, \delta\}$
15: **end for**
16: **until** *Maximum Var*(D_{path})
17: Updating physical layout

Meanwhile, for any register pin s'_i in set S'_{reg}, we calculate each path length $L(s_0, s'_i)$ from s_0 to s'_i by Manhattan distance $d_m(\cdot)$. Moreover, the related path delay set $D_{\text{path}} = \{T_{\text{Delay},i}\}$ is obtained based on the path length set L_{path} using the Elmore delay (see lines 13–16).

Convergence and Complexity: The security-driven placement described in Algorithm 1 is a numerical optimization method that obtains the relative optimum solution by random searching. It terminates when the maximum iteration is met, and the placement with the maximum $\text{Var}(D_{\text{path}})$ is selected as the approximate optimum solution. Placement graph $G(V, E)$ is updated to acquire a new placement with optimum EM SCA resistance. In terms of the computation complexity, besides the iteration counts, the overall run time of Algorithm 1 is influenced by the circuit size, including the number of clock cells and data-dependent registers. The computation complexity in each iteration is dominated by resolving the overlapped regions (lines 6–12) which is $O(mn^2)$, where m and n are the number clock cells and data-dependent registers, respectively. Therefore, the computation complexity of Algorithm 1 is $O(qmn^2)$ with the total iteration number q.

B. Framework of CAD4EM-P: Security-Driven Routing

After the security-drive placement stage, CAD4EM-P will then optimize the routed design following steps in Algorithm 2. CAD4EM-P first judge whether the reallocation boundary exceeds the core area A_{CORE} of the given placement (see line 1). If the answer is yes, it will execute the security-driven routing by two steps, including routing channel analysis and data-dependent wire length adjustments.

Lines 2–10 describe the *routing channel analysis*. We extract the complete routing network R_{Net} which connects cells together using metal wires and vias. For each wire, its physical information containing coordinates, geometry, and subordinate layer can be obtained from the routed netlist. We denote the signal paths from the clock buffer to the clock port of data-dependent registers as data-dependent paths. Wires that are not in these paths are collected in the data-independent routing network R_{INet}. Under fixed R, we can acquire the feasible region to fill the data-dependent path, according to the geometry constraint. Meanwhile, its area A_{DR} in the N-layer layout can be calculated as

$$A_{\text{DR}} = N \times A_{\text{CORE}} - \sum_{i \in IR_{\text{Net}}} l_i \times (w_i + s_i) \tag{8}$$

where l_i, w_i, and s_i denote the length, width and spacing of the ith metal wire. Combined with the maximum routing length, the maximum length for extended data-dependent routing can be estimated.

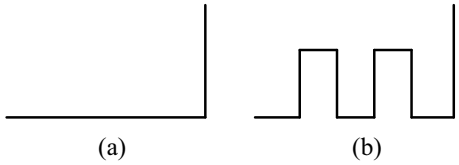


Fig. 4. (a) Regular wire. (b) Wire snaking.

Lines 11–16 describe the *data-dependent wire length adjustments*. Given the maximum path delay $D_{\max}$ and delay interval δ, we adjust the length of each wire in the data-dependent routing network R_{DNet}, under the above constraints. This adjustment is realized by wire snaking, which is a popular approach to incur useful wire delays, as mentioned in Section II-A. Fig. 4 shows a comparison between regular wire and wire snaking. We turn the metal wires in either of left, right, up, or down directions to increase routing length and avoid obstacles and antenna effect. In this way, we further improve the circuit's resistance against EM SCA attacks.

Convergence and Complexity: During the optimization, existing routing may hinder wire length adjustments using wire snaking. This scenario happens for designs with high routing density. To solve this, CAD4EM-P divides the layout into integer-squared grids and the metal density is computed for each grid. Wire snaking is then applied to these data-dependent wires inside the grid with low metal density. Moreover, if the deviation is less than the delay interval, the wire after adjustment will be accepted as the approximate optimum solution. Hence, the security-driven routing in CAD4EM-P is guaranteed to terminate. In terms of the computation complexity, the algorithm has a $O(n)$ computation complexity, where n is the number of data-dependent wires (lines 12–16 in Algorithm 2).

C. Integrating CAD4EM-P to Existing Design Flow

As shown in Fig. 5, 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 $G(V, E)$ 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

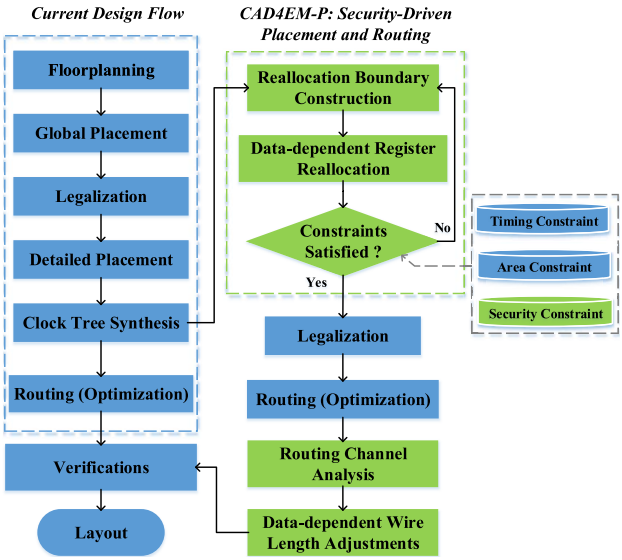


Fig. 5. CAD4EM-P integration to the current design flow.

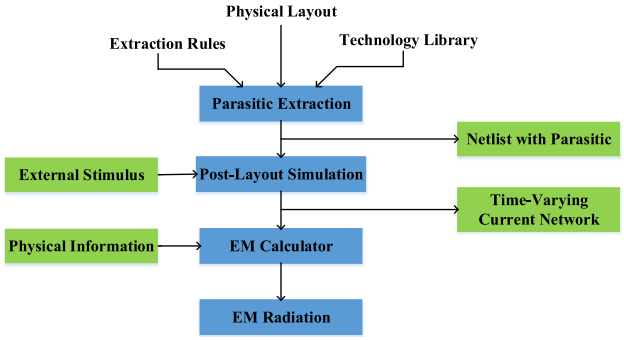


Fig. 6. Layout-level EM simulation flow.

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, generating a list that consists of feasible register locations. Delay computation is also performed and the obtained Var(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 corresponding 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 reimported to the layout design tool and legalization is performed again to remove these introduced cell overlaps. Then, the existing routing tool will connect all components of the new placement with vertical and horizontal wires. For this routed layout, CAD4EM-P will parse the new design file, i.e., *design.def*, to build the whole routing channel. According to user-defined registers, the relevant wires are selected and their feasible routing region is computed. Given user-defined $D_{\max}$ and δ, CAD4EM-P will generate the scheme for wire length adjustments based on the principle of minimum adjustment and maximum Var(D_{path}). Finally, the layout with optimum EM SCA resistance is generated by optimization and verification processes in the existing design flow.

D. Layout-Level EM Simulation Flow

Considering the requirement for evaluating the EM leakage during IC layout design flow, the layout-level simulation method in [37] is utilized. This type of method has been validated in [38], where a good agreement between the simulated EM radiation and measured data exists. Fig. 6 shows the overall flow of the layout-level EM simulation. We first extract layout-level parasitics after passing the layout versus schematic (LVS) checking. The parasitic extractor, i.e., Calibre xRC, makes use of the layout data (*design.gds*) to calculate its inner parasitic resistance and capacitance. In this process, The transistor-level type is selected for better extraction accuracy. A parasitic netlist (*design.dspf*) will be reported by the extractor in the DSPF format. Then HSPICE annotates extracted parasitic elements to the ideal SPICE netlist (*design.sp*) of the design for post-layout simulation. Through transistor-level simulation, transient currents that flow within all metal wires are obtained. Meanwhile, physical information of each metal wire can be gained by interpreting the parasitic netlist, including actual location, width, length, and layer. Combing these, we can construct a time-varying current network based on the structural attributes of the layout. Finally, EM emissions from every point of the IC's surface to any observer point can be computed through the superposition principle, as shown in (2).

V. Experimental Results on Simplified AES Designs

In this section, we will first validate the developed EM leakage model utilizing layout-level EM simulation methodology. Then we provide experimental proofs to demonstrate the efficacy of the proposed CAD4EM-P tool on simplified AES designs. Please note that only security-driven placement is applied in this section. The complete effect of CAD4EM-P, containing both security-driven placement and routing will be discussed in Section VI.

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 [39]. 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 the 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

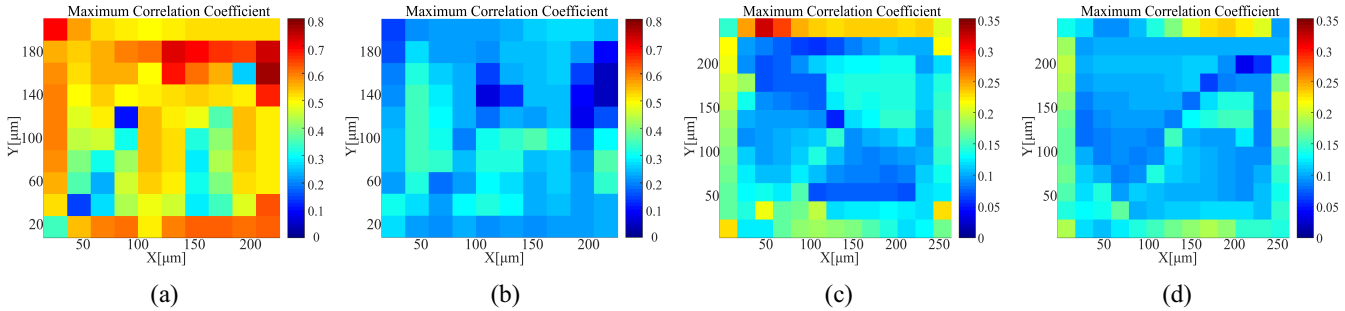


Fig. 7. EM information leakage maps of (a) nonprot. AES-GF, (b) prot. AES-GF, (c) nonprot. AES-LUT, and (d) prot. AES-LUT.

TABLE I
AVERAGE MAGNETIC FIELD AMPLITUDES FROM SIGNAL LINES VERSUS POWER GRIDS IN EACH METAL LAYER

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

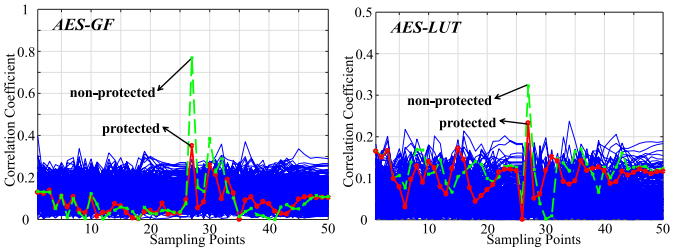


Fig. 8. CEMA results for EM leakage hot spots of (a) AES-GF and (b) AES-LUT.

data fetching from vast of memory results in high power consumption, denoted as AES-LUT. Their RTL descriptions are synthesized using SMIC 180-nm logic technology in Synopsys Design Compiler [40] and then placed and routed using Cadence SOC Encounter [41]. The physical layout consists of four metal layers, where Metal4 and Metal3 are used for global power routing and Metal1 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 nonprotected circuits, the only difference of the protected designs is that CAD4EM-P is applied to help generate the layout (see Fig. 5). The tool requires 19 min to execute 500 round iterations and generates an optimum placement on a platform with an Intel 1.60 GHz CPU with 8 GB memory.

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 $D = 30\ \mu$m to mimic the actual environment of localized EM SCA attacks [5], [6].

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×. Moreover, we construct EM information maps to compute the contribution of signal lines in the context of side-channel security according to (9). 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. 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

$$\text{Contribution} = \text{Avg.}\frac{\text{Leakage Matrix} \mid \text{signal}}{\text{Leakage Matrix} \mid \text{power} + \text{signal}}. \quad (9)$$

C. Efficacy of CAD4EM-P: Security-Driven Placement

Fig. 7 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 EM information leakage, in which the topmost color denotes that this point leaks maximum EM information that can be exploited by an attacker. Evidently, the EM information leakage is significantly reduced compared with nonprotected 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 Fig. 8, where red and green traces denote the correlation of the correct key of the nonprotected 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 nonprotected 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 wire length causes higher power consumption.

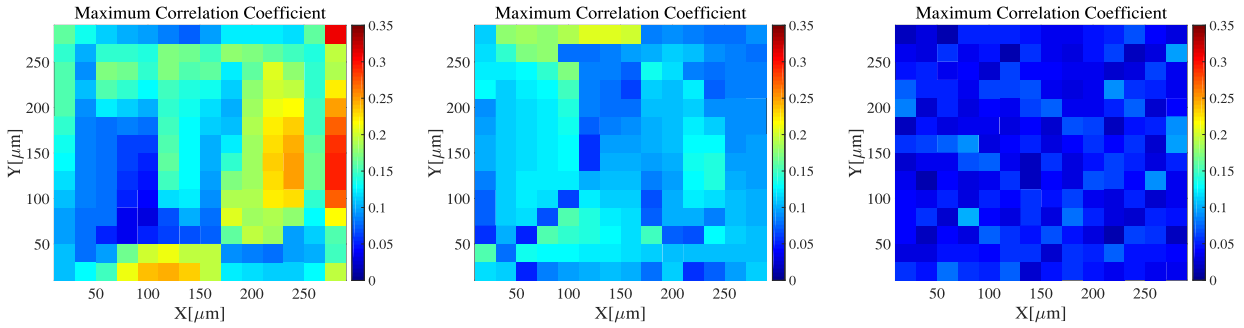


Fig. 9. EM information leakage maps of (a) AES-128 without protection, (b) AES-128 with placement optimization only, and (c) AES-128 with placement and routing optimization.

TABLE II
BALANCE OF SECURITY AND 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.
† Prot. denotes the placement optimization caused by the CAD4EM tool.

VI. EXPERIMENTAL RESULTS ON AES-128 AND PRESENT

Besides simplified AES designs, we further validate the efficacy of CAD4EM-P on medium-scale cryptographic circuits, including AES-128 and PRESENT cores to prove the scalability of the designed CAD4EM-P tool. Both security-driven placement and routing will be performed and their effectiveness will be verified.

A. Target Designs

AES-128 Core: This complete version of the AES circuit encrypts 128-bit plaintext using cipher keys with a length of 128 bits, denoted as AES-128. Before encryptions, a KeySchedule block is used to expand the key into round keys. Then AES-128 executes through ten rounds of encryptions and each round comprises four operations: 1) SubBytes; 2) ShiftRows; 3) Mixcolumns (except for the last round); and 4) AddRoundKey. In each round, four S-Boxes are performed serially occupying four clock cycles while other operations are completed in the next cycle. State registers are exploited to store intermediate data and output ciphertexts. Plaintexts and keys are loaded via a universal asynchronous receiver-transmitter (UART) block.

PRESENT Core: This lightweight block cipher encrypts the 64-bit block using 80-bit keys [42]. PRESENT consists of 31 rounds and each round has an XOR operation, a linear bit-wise permutation, and a nonlinear substitution layer. This nonlinear layer is implemented by the single 4-bit SBox which executes 16 times concurrently in one round. The intermediate data are stored in state registers. Also, we use an UART block to transmit plaintexts and keys.

The RTL descriptions of AES-128 and PRESENT are transformed into the final layouts using SMIC 180-nm technology, consisting of four metal layers. Their clock frequency and the supply voltage are 20 MHz and 1.8 V, respectively. The developed CAD4EM-P is applied to secure both designs. More specifically, the protection is twofold. First, state registers after S-Boxes are selected as data-dependent registers and pass through security-driven placement. Second, wires that connect the clock buffers and data-dependent registers are selected as data-dependent wires and pass through security-driven routing.

B. Efficacy of CAD4EM-P: Security-Driven Placement

To perform localized EM SCA attacks, we implement both AES-128 and PRESENT designs into square networks in which each grid has a side length of about 20 μm. For probe height 30 μm, EM emissions on each grid are simulated while circuits encrypt 1000 plaintexts consecutively. Then CEMA attacks are performed to construct the EM information map, through scanning the whole surface.

1) AES-128 Core: Since AES-128 performs pipelined 32-bit S-Box operations, the attack scenarios are similar on all these four S-Boxes. In our experiments, we chose the first 32-bit S-Box operation as the attack target. Regions of the information leakage maps are shown in Fig. 9(a) and (b), including hot spots that leak the highest degree of sensitive information. As shown, after optimizing the placement of AES-128 with CAD4EM-P, the EM information leakage of the hot spot is reduced with the maximum correlation decreasing by 36.59%. Meanwhile, Fig. 10 shows the CEMA attack results on the hot spot of the AES-128 design. These results depict the evolution of maximum correlations of hypothetical keys, with increasing number of traces N_{trace}. Among them, the red curve represents the correct hypothesis of the secret key. The minimum traces to disclosure the key is denoted as N_{MTD}. When $N_{\text{trace}} > N_{\text{MTD}}$, the correlation waveform for the correct hypothesis will always be above those for the wrong hypotheses. $N_{\text{MTD}} \approx 120$ for nonprotected design as shown in Fig. 10(a), while $N_{\text{MTD}} \approx 633$ after applying security-driven placement as shown in Fig. 10(b). This means that CAD4EM-P can boost the security of AES-128 by at least 5×.

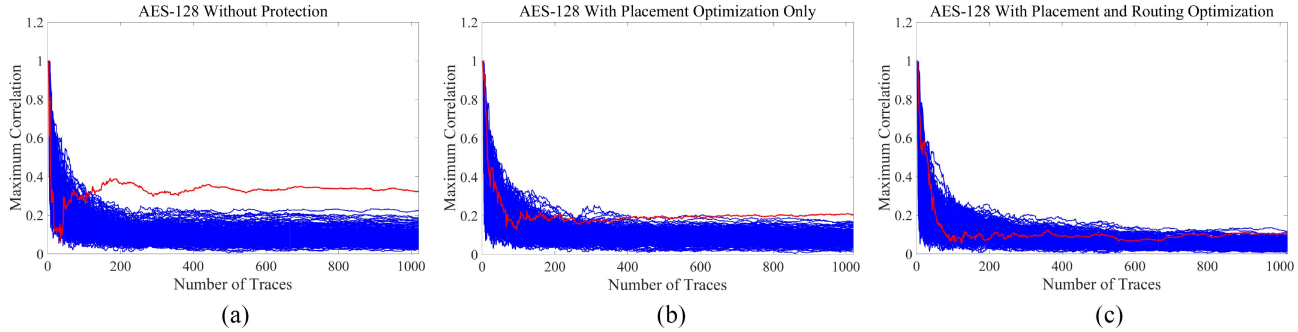


Fig. 10. CEMA attack results on the hot spot of (a) AES-128 without protection, (b) AES-128 with placement optimization only, and (c) AES-128 with placement and routing optimization.

TABLE III
BALANCE OF SECURITY AND OVERHEADS

Target Design	AES-128			PRESENT		
	Without Protection	Placement Optimization Only	Placement and Routing Optimization	Without Protection	Placement Optimization Only	Placement and Routing Optimization
Clock Skew (ns)	0.043	0.63	2.972	0.027	0.428	2.50
Total Area (μm^2)	1690780	1690780	1690780	882264	882264	882264
Wire Length	34391	68533	89584	13728	24950	40766
Average Power (mW)	3.54	3.92	4.14	1.70	1.88	2.09
Maximum Correlation	0.3222	0.2043	0.1055	0.5564	0.3999	0.1081

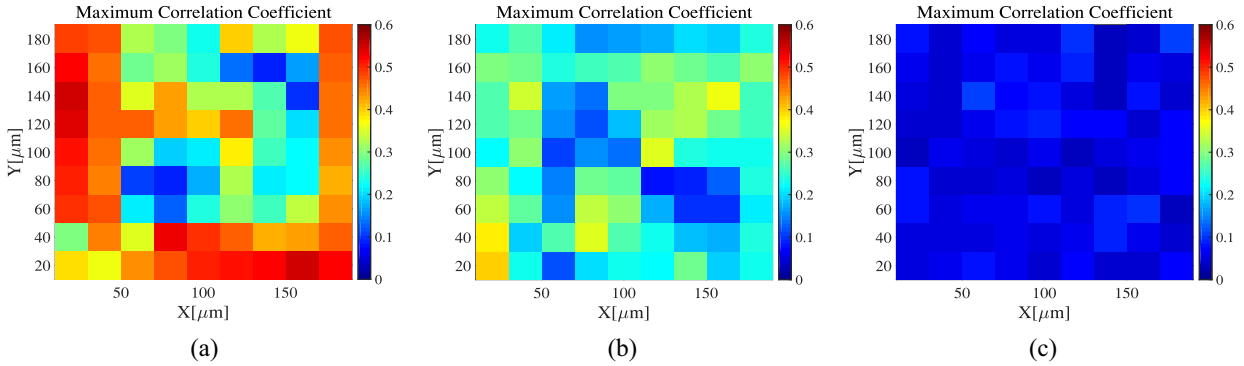


Fig. 11. EM information leakage maps of (a) PRESENT without protection, (b) PRESENT with placement optimization only, and (c) PRESENT with placement and routing optimization.

Table III summarizes the overhead of security-driven placement in CAD4EM-P on AES-128 design, including timing, area, and power overheads. We denote the maximum deviation of clock delay between the clock source and data-dependent registers as T_{skew}. $T_{\text{skew}} = 0.043$ ns and $T_{\text{skew}} = 0.63$ ns for AES-128 design before and after placement optimization, showing an efficient result on breaking the balanced T_{skew}. Meanwhile, we find that the increased skews do not introduce timing violations since the design satisfies entire timing constraints. CAD4EM-P will not alter the actual die size as the security-oriented optimizations are confined to the given core area. Due to incremental T_{skew}, the wire length of the clock network increases, and thus results in an augment of the average power by 10.73%.

2) PRESENT Core: In PRESENT, S-Box is the only nonlinear operation that guarantees its confusion and diffusion. The moment when PRESENT executes S-Box operations is commonly considered as the attack target. Fig. 11(a) and (b) show the information leakage of regions that embrace hot spots before and after placement optimization. For the protected hot spot, leaked EM information is reduced with the maximum correlation decreasing by 28.13%. More specifically, The trend of maximum correlations over the number of traces is shown in Fig. 12. Compared to the original $N_{\text{MTD}} \approx 75$, $N_{\text{MTD}} \approx 375$ can be achieved under protection as shown in Fig. 12(b).

The overahead of CAD4EM-P on PRESENT design is also shown in Table III. After placement optimization by CAD4EM-P, T_{skew} increases from 0.027 to 0.428 ns. Within the same die size, the average power consumption increase by 10.59% due to the increased wire length.

C. Efficacy of CAD4EM-P: Security-Driven Routing

In this section, we validate the efficacy of the security-driven routing in the CAD4EM-P tool as discussed in Section IV-B.

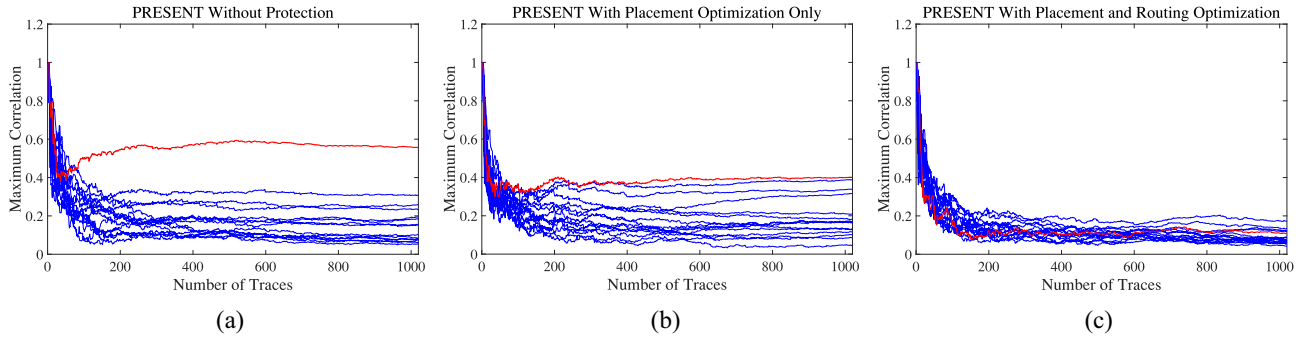


Fig. 12. CEMA attack results on the hot spot of (a) PRESENT without protection, (b) PRESENT with placement optimization only, and (c) PRESENT with placement and routing optimization.

In Cadence SoC Encounter, we increase the wire length of data-dependent wires using wire length adjustments. The updated layout passed through all verifications successfully, including geometry, connectivity, and timing. Note that the security-driven routing is applied to designs with placement optimization to further improve the EM SCA resistance. Hence, we compare the EM SCA resistance of final layouts to these carrying only placement optimization. Through layout-level EM simulation, localized EM SCA attacks are performed and the information leakage maps are shown in Figs. 9(c) and 11(c). Meanwhile, attack results on hot spots are shown in Figs. 10(c) and 12(c). For AES-128, $N_{\text{MTD}} > 1000$ is realized with the maximum correlation decreasing by 48.36%. As shown in Table III, T_{skew} is 2.972 ns and the average power increases to 4.14 mW after using routing optimizations. For PRESENT, the routing strategy promotes N_{MTD} to more than 1000 and decreases the maximum correlation to 0.1081. Accordingly, T_{skew} and the average power are 2.50 ns and 2.09 mW, respectively, due to the increased wire length.

D. Robustness Verification of CAD4EM-P

In this section, we investigate the robustness of the developed CAD4EM-P under preprocessing-based CEMA attacks. We refer pure CEMA attacks on the EM traces of nonprotected and protected designs as CEMA-NPD and CEMA-PD, respectively. For protected designs, once the EM traces of hot spots are collected, SA, EA, FFT, or PCA algorithm is carried out and CEMA attacks are performed on these preprocessed EM traces. Hence, we refer CEMA attacks on the protected EM traces preprocessed by SA algorithm, EA algorithm, FFT algorithm, and PCA algorithm as SA-CEMA, EA-CEMA, FFT-CEMA, and PCA-CEMA, respectively (see Fig. 13).

For all the mentioned designs, the maximum correlations of the correct key under the above attack scenarios are shown in Fig. 13. As shown, the correlations between EM traces and the processed data are significantly reduced after applying CAD4EM-P, which is analyzed in the above sections. Moreover, maximum correlations are slightly altered under SA-CEMA, EA-CEMA, and PCA-CEMA attacks, and in particular, are reduced observably under the FFT-CEMA attack. These results show that both alignment and

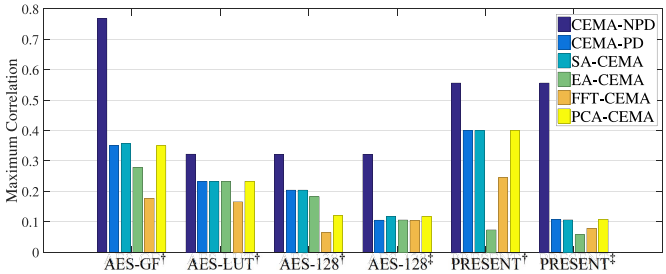


Fig. 13. Robustness verification of CAD4EM-P: NPD and PD denote the nonprotected and protected designs, respectively. For those designs under protection, † denotes circuit with placement optimization only, and ‡ denotes circuit with placement and routing optimizations.

transformation-based preprocessing analysis fail to reduce the security of designs optimized by CAD4EM-P. CAD4EM-P only randomizes the distribution of EM leakage from data-dependent registers, which are subcomponents for total EM radiation. SA and EA algorithms cannot determine adequate patterns to align these inner randomizations. Moreover, because randomized EM leakage from data-dependent registers will overlap with those from other parts together, FFT and PCA algorithms cannot remove the above randomness. Therefore, it is validated that the CAD4EM-P can withstand these preprocessing-based attacks.

VII. Conclusion

In this article, we proposed a CAD for security tool CAD4EM-P to consider security attributes within the modern IC design flow against EM SCA attacks. The key idea is derived from the observation that the amount of EM leakage mostly comes from power grids while its temporal distribution is regulated by placement and routing. CAD4EM-P helps optimize the initial layout to maximize EM leakage deviation by two successive stages, including solving the security-driven placement and routing problems. Utilizing the EM simulation method at the layout-level, experiment results show that CAD4EM-P can secure different versions of AES and PRESENT circuits against EM SCA attacks, with reasonable area and power overheads. In our future work, we will investigate and develop more CAD for security tools for circuit protection in an automatic way.

REFERENCES

[1] 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.

[2] L. Zhang, D. Mu, W. Hu, Y. Tai, J. Blackstone, and R. Kastner, "Memory-based high-level synthesis optimizations security exploration on the power side-channel," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 39, no. 10, pp. 2124–2137, Oct. 2020.

[3] 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. Orient. Secur. Trust Symp. (AsianHOST)*, 2019, pp. 1–6.

[4] J. Heyszl, D. Merli, B. Heinz, F. D. Santis, and G. Sigl, "Strengths and limitations of high-resolution electromagnetic field measurements for side-channel analysis," in *Proc. Int. Conf. Smart Card Res. Adv. Appl.*, 2012, pp. 248–262.

[5] V. Immler, R. Specht, and F. Unterstein, "Your rails cannot hide from localized EM: How dual-rail logic fails on FPGAs," in *Proc. Int. Conf. Cryptogr. Hardw. Embedded Syst.*, 2017, pp. 403–424.

[6] R. Specht, V. Immler, F. Unterstein, J. Heyszl, and G. Sig, "Dividing the threshold: Multi-probe localized EM analysis on threshold implementations," in *Proc. IEEE Int. Symp. Hardw. Orient. Secur. Trust (HOST)*, 2018, pp. 33–40.

[7] 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. Orient. Secur. Trust*, 2019, pp. 11–20.

[8] A. B. Kahng, J. Lienig, I. L. Markov, and J. Hu, *VLSI Physical Design: From Graph Partitioning to Timing Closure*. Dordrecht, The Netherlands: Springer, 2011.

[9] S. Batterywala, N. Shenoy, W. Nicholls, and H. Zhou, "Track assignment: A desirable intermediate step between global routing and detailed routing," in *Proc. IEEE/ACM Int. Conf. Comput. Aided Design*, 2002, pp. 59–66.

[10] Y. Cheon, P.-H. Ho, A. B. Kahng, S. Reda, and Q. Wang, "Power-aware placement," in *Proc. 42nd Design Autom. Conf.*, 2005, pp. 795–800.

[11] Y. Lu *et al.*, "Navigating registers in placement for clock network minimization," in *Proc. 42nd Design Autom. Conf.*, 2005, pp. 176–181.

[12] G. Wu, Y. Xu, D. Wu, M. Ragupathy, Y.-Y. Mo, and C. Chu, "Flip-flop clustering by weighted K-means algorithm," in *Proc. 53rd Annu. Design Autom. Conf.*, 2016, p. 82.

[13] I.-M. Liu, T.-L. Chou, A. Aziz, and D. F. Wong, "Zero-skew clock tree construction by simultaneous routing, wire sizing and buffer insertion," in *Proc. Int. Symp. Phys. Design*, 2000, pp. 33–38.

[14] J.-L. Tsai, T.-H. Chen, and C. C.-P. Chen, "Zero skew clock-tree optimization with buffer insertion/sizing and wire sizing," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 23, no. 4, pp. 565–572, Apr. 2004.

[15] M. R. Guthaus, D. Sylvester, and R. B. Brown, "Clock buffer and wire sizing using sequential programming," in *Proc. 43rd Annu. Design Autom. Conf.*, 2006, pp. 1041–1046.

[16] R.-S. Tsay, "An exact zero-skew clock routing algorithm," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 12, no. 2, pp. 242–249, Feb. 1993.

[17] R. Chaturvedi and J. Hu, "Buffered clock tree for high quality IC design," in *Proc. Int. Symp. Signals Circuits Syst. (SCS)*, 2004, pp. 381–386.

[18] Y.-Y. Chen, C. Dong, and D. Chen, "Clock tree synthesis under aggressive buffer insertion," in *Proc. 47th Design Autom. Conf.*, 2010, pp. 86–89.

[19] W. Liu, C. Sitik, E. Salman, B. Taskin, S. Sundareswaran, and B. Huang, "SLECTS: Slew-driven clock tree synthesis," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 27, no. 4, pp. 864–874, Apr. 2019.

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

[21] A. A. Pammu, K.-S. Chong, and B.-H. Gwee, "Highly secured arithmetic hiding based S-box on AES-128 implementation," in *Proc. Int. Symp. Integr. Circuits (ISIC)*, 2016, pp. 1–4.

[22] F. Poucheret, L. Barthe, P. Benoit, L. Torres, P. Maurine, and M. Robert, "Spatial EM jamming: A countermeasure against EM analysis?" in *Proc. 18th IEEE/IFIP Int. Conf. VLSI Syst. Chip*, 2010, pp. 105–110.

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

[24] M. Kar *et al.*, "Blindsight: Blinding EM side-channel leakage using built-in fully integrated inductive voltage regulator," 2018. [Online]. Available: arXiv:1802.09096.

[25] 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 J. Solid-State Circuits*, vol. 54, no. 2, pp. 569–583, Feb. 2019.

[26] D. B. Roy, S. Bhasin, S. Guilley, J.-L. Danger, and D. Mukhopadhyay, "From theory to practice of private circuit: A cautionary note," in *Proc. 33rd IEEE Int. Conf. Comput. Design (ICCD)*, 2015, pp. 296–303.

[27] 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 Pac. Design Autom. Conf. (ASP-DAC)*, 2020, pp. 62–67.

[28] S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks: Revealing the Secrets of Smart Cards*, vol. 31. Berlin, Germany: Springer, 2008.

[29] J. G. van Woudenberg, M. F. Witteman, and B. Bakker, "Improving differential power analysis by elastic alignment," in *Proc. Cryptogr. Track RSA Conf.*, 2011, pp. 104–119.

[30] E. Mateos and C. H. Gebotys, "A new correlation frequency analysis of the side channel," in *Proc. 5th Workshop Embedded Syst. Secur.*, 2010, pp. 1–8.

[31] J. Hogenboom and L. Batina, "Principal component analysis and side-channel attacks," M.S. thesis, Dept. Comput. Sci. Dig. Security, Radboud University Nijmegen, Nijmegen, The Netherlands, 2010.

[32] K. Gala, V. Zolotov, R. Panda, B. Young, J. Wang, and D. Blaauw, "On-chip inductance modeling and analysis," in *Proc. 37th Annu. Design Autom. Conf.*, 2000, pp. 63–68.

[33] 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 Trans. Electromagn. Compat.*, vol. 47, no. 3, pp. 424–439, Aug. 2005.

[34] Y. Lu, M. O'Neill, and J. McCanny, "Evaluation of random delay insertion against DPA on FPGAs," *ACM Trans. Reconfigurable Technol. Syst.*, vol. 4, no. 1, pp. 1–20, 2010.

[35] J. Lu, W.-K. Chow, and C.-W. Sham, "Fast power-and slew-aware gated clock tree synthesis," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 20, no. 11, pp. 2094–2103, Nov. 2012.

[36] Z.-W. Chen and J.-T. Yan, "Routability-driven flip-flop merging process for clock power reduction," in *Proc. IEEE Int. Conf. Comput. Design*, 2010, pp. 203–208.

[37] 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.

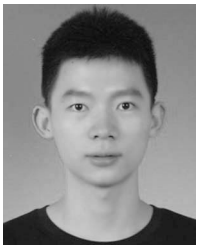
[38] V. Lomné, P. Maurine, L. Torres, T. Ordas, M. Lisart, and J. Toublanc, "Modeling time domain magnetic emissions of ICs," in *Proc. Int. Workshop Power Timing Model. Optim. Simulat.*, 2010, pp. 238–249.

[39] X. Wang *et al.*, "Role of power grid in side channel attack and power-grid-aware secure design," in *Proc. 50th Annu. Design Autom. Conf.*, 2013, p. 78.

[40] Synopsys Inc. *Design Compiler*. Accessed: Mar. 20, 2020. [Online]. Available: https://www.synopsys.com

[41] Cadence Inc. *SOC Encounter*. Accessed: Mar. 20, 2020. [Online]. Available: https://www.cadence.com

[42] A. Bogdanov *et al.*, "PRESENT: An ultra-lightweight block cipher," in *Proc. Int. Workshop Cryptogr. Hardw. Embedded Syst.*, 2007, pp. 450–466.



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.

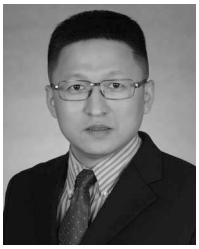
His current research interests include digital circuit design, hardware security, and EDA for security.

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, Tianjin, China, in 2013, 2015, and 2019, respectively.

He was a Visiting Scholar with the University of Central Florida, Orlando, FL, USA, and the University of Florida, Gainesville, FL, USA, from 2016 to 2018. He is currently a Postdoctoral Research Fellow with the Institute of Microelectronics, Tsinghua University, Beijing, China. His research interests are digital circuit design, hardware security, and EDA for security.

Yanjiang Liu received the M.S. degree in circuits and systems from the Guangdong University of Technology, Guangzhou, China, in 2016, and the Ph.D. degree from the School of Microelectronics, Tianjin University, Tianjin, China, in 2020.

His current research interests include digital circuit design and hardware security.



Leibo Liu (Senior Member, IEEE) received the B.S. degree in electronic engineering and the Ph.D. degree from the Institute of Microelectronics, Tsinghua University, Beijing, China, in 1999 and 2004, respectively.

He is currently a Full Professor with the Institute of Microelectronics, Tsinghua University. His current research interests include reconfigurable computing, mobile computing, and very large-scale integration digital signal processing.

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 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, Hangzhou, China, in 2005 and 2007, respectively, and the Ph.D. degree in electrical engineering from Yale University, New Haven, CT, USA, in 2012.

He is an Associate Professor and an IoT Term Professor with the Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL, USA. His research focuses on the areas of hardware security, embedded systems design and security, trusted hardware intellectual property cores, and hardware-software co-design for modern computing systems. He is also interested in the security analysis on Internet of Things (IoT), wearable devices with particular emphasis on information integrity, and privacy protection in the IoT era.

Dr. Jin is a recipient of the DoE Early CAREER Award in 2016, the ONR Young Investigator Award in 2019, and the Best Paper Award at DAC'15, ASP-DAC'16, HOST'17, ACM TODAES'18, GLSVLSI'18, and DATE'19. He is also the IEEE Council on Electronic Design Automation Distinguished Lecturer.