Automatic On-Chip Clock Network Optimization for Electromagnetic Side-Channel Protection

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

***Abstract*— Commercial electronic design automation (EDA) tools typically focus on optimizing the power, area, and speed of integrated circuits (ICs). They rarely consider hardware security requirements. As such, existing EDA tools often directly or indirectly introduce security vulnerabilities. These security vulnerabilities can later be exploited by attackers to leak information or compromise the hardware root-of-trust. In this paper, we show how traditional EDA tools optimize power, area and speed (PAS) metrics in cryptographic circuits at the cost of introducing vulnerabilities to side-channel analysis (SCA) attacks. To balance hardware security with traditional performance metrics, we propose an automatic tool, called CAD4EM-CLK, to secure ICs against power and electromagnetic (EM) SCA attacks. The tool optimizes clock networks for both traditional design requirements and security constraints. To achieve this goal, we first theoretically analyze and model the relationship between on-chip clock networks and side-channel security. The developed model will then guide the CAD4EM-CLK tool to adjust clock network structures to spread the leakage out temporally, also lower its amplitude proportion, so as to help reduce the leaked information. The proposed automatic tool is then validated on various cryptographic circuits. We use layout-level simulation to assess side-channel leakage and the experimental results prove the effectiveness of our proposed tool for power and EM side-channel protection.**

***Index Terms*— CAD for security, side-channel attack, electromagnetic leakage, power side channel, clock tree synthesis.**

I. Introduction

As THE hardware foundation of modern electronic systems, integrated circuits (ICs) are required to satisfy certain power, area, speed, and security (PASS) requirements. Since IC designs become increasingly complex, designers have to rely on state-of-the-art electronic design automation (EDA) tools to achieve PAS restrictions. However, security is rarely a constraint in the traditional IC design flow [1]. As a consequence, neither IC designers nor commercial EDA tools are well prepared for hardware security threats, resulting in ICs vulnerable to various hardware attacks [2], [3]. While hardware security education and training in recent years have helped cultivate a generation of designers with the appropriate background to take on these threats, the EDA industry as a whole is still not prepared to counter hardware threats. To further complicate matters, EDA tools themselves contribute to hardware vulnerabilities, either directly or indirectly. As such, the development of Computer Aided Design (CAD) tools for security is an urgent task for the hardware security community. In this paper, we will demonstrate their limitations and the enhancement of commercial EDA tools for hardware security, specifically for defending against SCA attacks.

SCA attacks represent one of the most critical hardware security risks. SCA leverages unavoidable physical manifestations from electronic devices that are relevant to the internal data processing. Specifically, that these manifestations can be exploited to extract sensitive information. Side-channel leakages often include power consumption, timing delay, as well as electromagnetic (EM) emanation.Among all side channels, EM emanation is derived from current flows inside ICs' metal wires, which carry information leaked by logic cells. This type of side channel has the advantage on the spatial domain and can be collected through a contactless way. Note that some EM side channel collection may need to decapsulate the chip to achieve a high signal-to-noise ratio (SNR). These properties make EM-based SCA attacks more powerful than other SCA attacks. EM SCA can be done with commercial components, and there are even public implementations available [4]. Further, other side channels such as the power side channel is caused by the presence of logic cells and hence has similar sources of side-channel leakage as the EM side channel. This gives us an opportunity to protect them by optimizing logic cells [5]. Thus, enhancing EM SCA resilience becomes one of the most important considerations when we redesign the IC design flow to include security as a metric.[1]

Researchers have proposed numerous countermeasures, often at the design level, that are classified into masking and hiding types. Masking techniques try to obfuscate the

Manuscript received December 13, 2020; revised February 22, 2021 and April 25, 2021; accepted April 27, 2021. Date of publication May 5, 2021; date of current version June 14, 2021. This article was recommended by Guest Editor N. Karimi. *(Corresponding author: Yiqiang Zhao.)*

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

Jiaji He is with the Institute of Microelectronics, Tsinghua University, Beijing 100084, China (e-mail: jiaji_he@mail.tsinghua.edu.cn).

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

Color versions of one or more figures in this article are available at https://doi.org/10.1109/JETCAS.2021.3077842.

Digital Object Identifier 10.1109/JETCAS.2021.3077842

[1]Due to the presence of the logic cells, EM side channel and power side channel have similar sources of side-channel leakage. Despite the differences between these two side channels, our method can apply to both EM side-channel and power side-channel protections since our work optimizes the leakage of logic cells by adjusting clock network. For simplicity, we will only discuss the EM side channel in detail. Simulation results on both EM and power side channel protections are presented in Section V and Section VI, respectively.

internal data such that the dependency between the sensitive information and the EM side-channel leakage can be eliminated [6]–[8]. Hiding represents a group of techniques aiming at reducing the information relativity of EM side-channel leakage. They can be implemented through randomizing the switching behaviors [9]–[11], attenuating EM emanations of sensitive blocks [12]–[14], injecting noise components [10], [15], [16], etc. However, in addition to significant power, area and speed overhead increases, these countermeasures require designers to have sufficient hardware security background to implement them correctly. A good example of this is [13], which greatly increases an AES design's security, but which has an area overhead of 22.85% and a power overhead of 49%, and requires extensive fine-tuning of a design. This requirement, combined with the lack of dedicated CAD tools, makes adoption of existing solutions difficult in the current IC design flow.

To address these deficiencies and, more importantly, to make side-channel security a metric similar to traditional performance metrics, we try to incorporate security constraints into modern EDA flows with our newly developed CAD for Security tools. In this way, we will achieve two goals. First, we seek to implement a defense that does not require a designer to have a comprehensive understanding of hardware security threats. And secondly, that this defence still allows for optimization among all PASS metrics.

Our work is based on the finding that the *Clock Tree Synthesis* (CTS) process in modern EDA flows tries to optimize power, area and speed metrics by sacrificing security (even under cases that all PAS metrics have been met). CTS generates the clock network which provides clock signals for sequential components, e.g., flip-flops (FFs). The features of the clock network and linked components will affect the time and amplitude characteristics of exploitable side-channel leakages. Take clock skew (defined in Section II-A) for instance, as clock skew is minimized, the time at which various components may be handling sensitive data become more temporally aligned. This temporal alignment causes any side channel leakage from the components to increase. Thus as CTS optimizes clock skew to the highest degree possible, past the minimum PAS requirements, it decreases the robustness of a design against SCA. To remedy this, we develop a CAD for Security tool, named CAD4EM-CLK, that performs optimizations for clock signal distribution, including clock tree and triggered registers, in order to quantitatively balance all user-specified PASS constraints. We then perform layout-level power and EM simulations on representative cryptographic hardware, the results of which demonstrate that the developed CAD4EM-CLK tool can protect circuit designs from SCA attacks with trivial PAS overheads. It is important to note that CAD4EM-CLK can be easily integrated with a number of other countermeasures techniques, and allows for designers to balance security and performance.

This paper has the following contributions to the hardware security and EDA communities.

- Theoretical proofs are provided to demonstrate that modern EDA tools contribute to power and EM side-channel vulnerabilities.
- A side-channel security metric is presented to quantitatively measure a circuit's resilience against power and EM side-channel attacks.
- We present a new approach to minimize the effects of side-channel leakage by spreading the leakage out temporally, also lowering its amplitude proportion.
- A new CAD for Security tool, named CAD4EM-CLK, is developed to leverage all of the above contributions. This tool allows a designer to achieve user-specified constraints of all design metrics, i.e., power, area, speed and side-channel security.

The rest of the paper is organized as follows. The required background is introduced in Section II. Section III models the security quality for design with the clock network, and theoretically analyzes the vulnerability of modern EDA tools on security requirements. Section IV discusses the overall framework of the proposed tool. Its effectiveness is validated in Section V and Section VI by simulation experiments. We conclude our work in Section VII.

II. Background

A. Clock Network Construction

The clock network is constructed to deliver clock signals within an IC, from the clock source to clock sinks, by connecting clock inputs of synchronous elements, e.g., Flip-Flops (FFs). The performance of a clock network will be evaluated from various objectives which are listed as follows.

- The clock latency is defined as the timing delay from the clock source to the sinks.
- The clock skew is defined as the difference in the arrival time of the clock signal traveling to two different sequential elements.
- The clock slew, or clock transition time, is defined as the time it takes for the signal to transition from one logic state to another.
- The clock power is defined as the total power consumption of the clock network.

To satisfy these objectives, different types of topological structures are applied to design the clock network, such as H-tree, buffered tree and clock mesh. Among them, buffered trees are the most popular in which buffers are inserted either at the clock source or the clock path. CTS is used to achieve these structures during EDA flow,. Also, it often implements various performance-driven optimization techniques to achieve the quality objectives mentioned above. For example, the authors in [17] present a clock-tuning algorithm involving buffer insertion to maintain the zero-skew property of the clock tree. Chen *et al.* guarantee the bounded clock slew of a clock tree through aggressive buffer insertion and minimizing the clock skew [18]. Liu *et al.* introduce the slew-driven approach (SLECTS) that considers slew optimizations at each phase of CTS [19]. Sitik *et al.* [20] propose a local clock gate cluster-aware low swing CTS method, in which low swing clocking is exploited for power consumption deduction while satisfying skew and slew constraints. In [21], the authors propose an improved K-means approach involving register clustering to reduce the power consumption.

B. CAD for Security Tools

EDA-friendly countermeasures and CAD for Security tools are attractive options for IC designers. In these solutions, security methods are either incorporated into the commercial design flow or developed as an open-source stand-alone tool so that designers no longer need to be proficient in both hardware design and side-channel security. In [22], [23], the authors present a secure design flow to flatten the power dissipation during each charge and discharge of the load capacitance. This is realized by building the secure logic library and adjusting place and route procedures. In [24], the authors propose an automatic design flow that pursues misaligned power dissipation. In this method, random clocks are introduced by code modification before logic synthesis. In [25], the authors develop security-driven synthesis methods for circuit protection.

Existing solutions try to embed generic countermeasures automatically, including random register switching, component masking, Boolean masking of data paths and their combinations. However, there is a lack of CAD tool for side-channel security enhancement optimizations. As demonstrated in [26] and theoretically proved in Section III-C, EDA algorithms often negatively impact the side-channel resistance of the design. In [26], the authors lower the power-based leakage by altering the parameter configuration on placed gate-level design, such as supply voltage, threshold voltage and gate size. In this paper, we develop a quantitative EM side-channel metric and incorporate it into the clock tree synthesis process. Thus, the side-channel security is assured along with other performance metrics.

C. Side-Channel Security Evaluation

To evaluate the security vulnerabilities of ICs, numerous methods have been proposed which include differential EM analysis (DEMA) [27], correlation EM analysis (CEMA) [28], mutual information analysis (MIA) [29] test-vector leakage assessment (TVLA) [30], etc. Among them, CEMA is widely used which exploits the Pearson correlation coefficient as an information indicator. This indicator quantifies the linear relation between actual EM traces T and the EM leakage model W, e.g., Hamming weight model [2] or Hamming distance model [31]. These models are used to predict the hypothetical EM side-channel behaviors of ICs executing cryptographic operations. Accordingly, the Pearson correlation coefficient is calculated in Equation (1) on each sampling point.

$$\rho\left(T, W\right) = \frac{E\left(T \cdot W\right) - E\left(T\right) \cdot E\left(W\right)}{\sqrt{Var\left(T\right) \cdot Var\left(W\right)}} \tag{1}$$

where $E(\cdot)$ and $Var(\cdot)$ are functions of calculating mean and variance of a set, respectively. The recovered key with the maximum Pearson correlation coefficient $\rho_{max} = max(\rho(T, W))$ indicates the most possible correct key.

III. EM Side Channel Modeling on Clock Network

A. EM Emanations Modeling

EM emanations originate from current flows within ICs. These flows are often caused by processing data, and as such, when critical data is being processed, EM leakage may occur. As illustrated in Figure 1(a), for a fabricated IC, the cell-level transistors on the silicon substrate, together with the wires and vias within multiple metal layers, constitute the basic current distribution topology [32]. The metal wires are divided into power grids and interconnect wires types. Using this model, we will try to identify the root cause of EM information leakage according to the propagation path. Specifically, we posit that transistor switching creates varying currents that emanate EM radiation into nearby space.

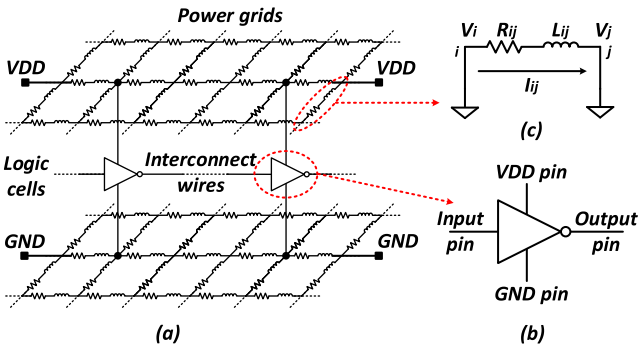

Fig. 1. (a) The current distribution topology of a CMOS IC [32] that includes (b) the standard cell and (c) metal wire.

This means transistors are the starting points that propagate information through the EM side channel. In CMOS-based circuits, a group of transistors with multiple pins form a standard cell that provides a Boolean function (e.g., AND, OR, XOR, INV) or a storage function (e.g., FF or latch). These pins are classified according to their functionality, either as input/output (I/O) pins or as power-supply pins. As shown in Figure 1(b), here we take an inverter for instance, the I/O pins are joined by interconnect wires, which transmit logic input or output signals between cells. Power-supply pins instead connect to power grids, such as VDD and GND, deliver positive and negative supply voltage to cells. When cells switch their output states, the shifting charge will draw current from the metal wires in their power grids, resulting in data-dependent currents. Furthermore, these power grids tend to have larger currents than the rest of the circuit, because they carry the supply and have a lower resistance than other wires [33].

In Figure 1(c), metal wires are separated into consecutive sections based on the vias' distribution. According to analysis in [34], we model each section as the π-type equivalent circuit. Logic cells that serve as excitation are modeled as independent current sources. Therefore, branch currents and node voltages of a segment can be calculated as Equation (2), according to the modified node analysis (MNA) [35].

$$\begin{aligned} G \cdot V + C\frac{\mathrm{d}V}{\mathrm{d}t} &= A \cdot I \\ I_{ij} &= \frac{V_i - V_j}{j\omega L_{ij} + R_{ij}} \end{aligned} \tag{2}$$

where $V, I \in \mathbb{R}^{n\times 1}$ are node voltages and currents over time, $G, C \in \mathbb{R}^{n\times n}$ are the conductance and capacitance matrices and $A \in \mathbb{R}^{n\times n}$ specifies where current sources are located.

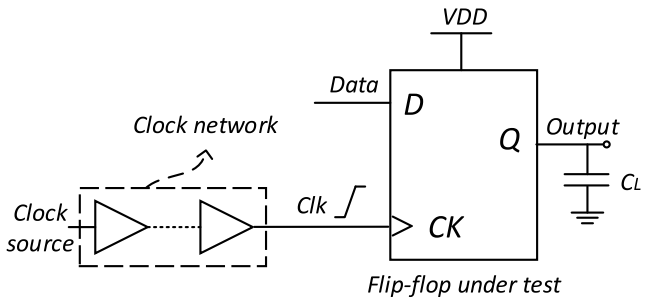

Fig. 2. Setup used to simulate the supply current.

R_{ij} and L_{ij} are wire resistance and inductance, ω is the angular frequency.

When carrying time-varying currents, metal wires start behaving as antennas and emit EM emanations. Let $J = I_{ij} \cdot \hat{v}$ denote the current density of the i-th segment, where $\hat{v}$ is the direction of the branch current I_{ij}. Through superposing contributions of all segments, the magnetic emanation from the IC can be computed in Equation (3).

$$B = \frac{\mu_0}{4\pi} \sum_{i \in all} \iint_{l_i \cdot w_i} \frac{J_i \times \hat{r_i}}{w_i r_i^2} ds \tag{3}$$

where l_i and w_i are the length and width of the i-th segment, respectively. r_i and $\widehat{r_i}$ are the magnitude and direction of the vector that is directed from the source point to the observer point. μ_0 is the magnetic permeability. Generally, EM emanation will be collected using external probes and the changing EM emanation will induce a voltage in the loop surface S_{probe} of the EM probe, as given as Equation (4).

$$V_{probe} = -\int_{S_{probe}} \frac{dB}{dt} \cdot ds \tag{4}$$

In this way, the collected EM emanation will have a relationship with critical information processed inside the circuit. Therefore, from Equations (2) to (4), it can be deduced that supply currents caused by cell switching are the information source of EM emanation from metal wires. Hence, optimizing the supply current in logic cells is vital in terms of EM side-channel security.

B. Flip-Flop Supply Current Modeling

Among all types of circuit cells, FFs are a major source of sensitive data leakage because FFs are driven by the clock network and thus synchronize the side-channel leakage [36]. So we will model the supply current in FFs considering the effect of clock slope and clock skew. These two parameters are the most important quality objectives when designing the clock network. Meanwhile, other influence factors like the type and output load will also be considered.

Figure 2 shows the setup used to test a generic FF under different clock conditions. This cell, named DFFHQ family in the standard cell library, is a high-speed, positive-edge triggered, static D-type FF. Note that the DFFHQ with asynchronous active-low reset, active-low set and both active-low set and reset are described as DFFRHQ, DFFSHQ and DFFSRHQ, respectively. The driven strength of these cells is labeled as X1, X2 and X4, in which a larger number means relatively higher capability to charge/discharge the output load.[2] Spice-level simulations are performed using a SMIC 0.18-μm process. The clock transition, clock arrival time and load capacitance are tuned to represent the variations of output load, clock slope and clock skew, respectively. To quantify their effects, we define three shape parameters of the supply current including peak current, peak time and pulse width. The peak current is the maximum amount of current in output-transition duration and its appearance point is defined as peak time. The pulse width is the time interval between points that located 10% up the rising edge and down the falling edge of the supply current.

Under all output-transition conditions, denoted as $TS = \{TS_1 : 0 \rightarrow 0,\ TS_2 : 1 \rightarrow 1,\ TS_3 : 1 \rightarrow 0,\ TS_4 : 0 \rightarrow 1\}$, the effect of clock slope, clock skew and load capacitance are shown in Figure 3. In Figure 3(a), the pulse width and peak time increase when smoothing the clock slope. The peak current is almost unaffected. In Figure 3(b), a smoother clock skew leads to linearly increased peak time. In Figure 3(c), the effect of load capacitance is output-transition type dependent. Under output transition TS_4, the load capacitance has a linear impact on the pulse width, while pulse width remains constant under other output transitions. Meanwhile, the effect of load capacitance on the peak current confines to output transition conditions TS_3 and TS_4.

Based on the above analysis, we formulate the supply current over time according to different output-transition conditions. For TS_1, TS_2, and TS_3 transitions, the load capacitance does not contribute to the pulse width. A two-term Gaussian function is established in Equations (6) to (9). Note that the value of many of these terms vary depending on how the FF's state is transitioning. For one type of FFs, i.e., DFFHQX2, fitting coefficients involved in these modeling formula can be found in Table I.

$$I_{FF}^{TS_j} = I_1^{TS_j} \cdot exp\left[-\frac{(t-t_1)^2}{\sigma_1^2}\right] + I_2 \cdot exp\left[-\frac{(t-t_2)^2}{\sigma_2^2}\right],\ j \in \{1,2,3\} \tag{5}$$

$$I_1^{TS_j} = \alpha_1 \cdot \tau_s + \alpha_2,\ j \in \{1,2\} \tag{6}$$

$$I_1^{TS_3} = \frac{K}{1 - exp[-g(C_l - C_m)]} \tag{7}$$

$$t_i = \beta_{i1} \cdot \tau_s + \tau_a + \beta_{i2},\ i \in \{1,2,p\} \tag{8}$$

$$\sigma_2 = \gamma_1 \cdot \tau_s + \gamma_2 \tag{9}$$

where τ_s, τ_a and C_l denote the clock slope, clock skew and load capacitance, respectively. For TS_4 transition, since the pulse width is influenced by load capacitance, we build a piecewise multi-term Gaussian function, in which the peak time t_p serves as the demarcation point. This function is given in Equations (10) to (13). The current curve before t_p is modeled as function I_r that has the same form as $I_{FF}^{TS_j}$, $j = \{1,2,3\}$. The current curve after t_p is represented as

[2]Note that different technology process libraries follow different gate naming rules. We follow the naming rule based on the target 0.18-μm process.

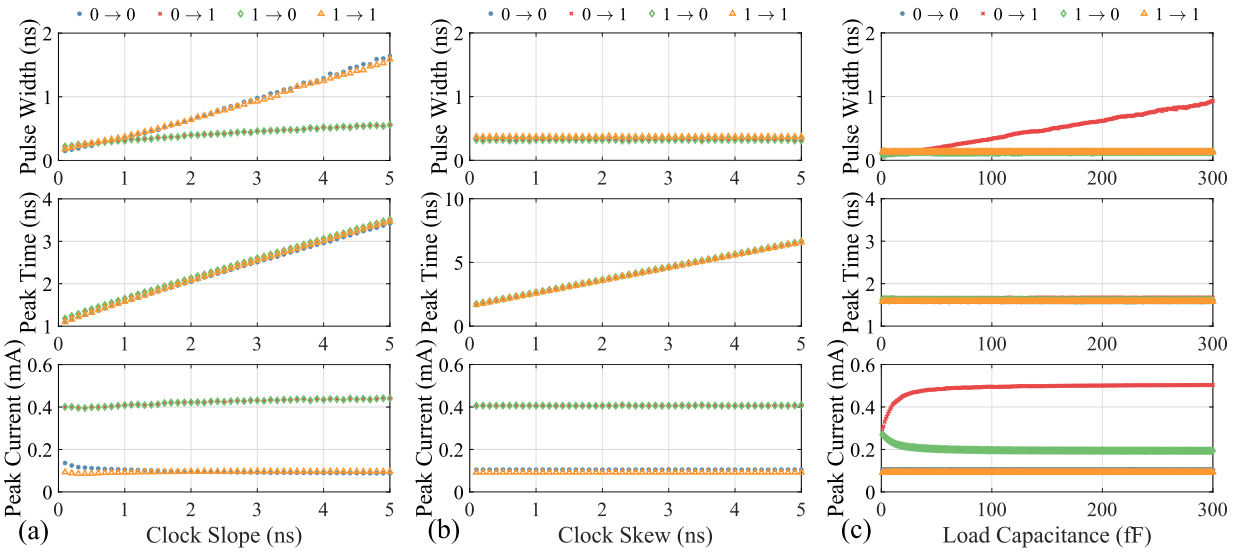

Fig. 3. The shape parameters of simulated (0.18-μm CMOS process) supply current in the FF versus (a) clock slope, (b) clock skew, and (c) load capacitance, under four-type output transitions.

a Gaussian function I_f, where I_p is the peak current calculated by I_r.

$$I_{FF}^{TS_4} = \frac{1 - sgn(t - t_p)}{2} \cdot I_r + \frac{1 + sgn(t - t_p)}{2} \cdot I_f \quad (10)$$

$$I_f = I_p \cdot exp\left[-\frac{(t - t_p)^2}{2\sigma_3^2}\right] \quad (11)$$

$$I_1^{TS_4} = \frac{K}{1 + exp[-g(C_l - C_m)]} \quad (12)$$

$$\sigma_3 = \lambda_1 \cdot C_l + \lambda_2 \quad (13)$$

Other fitting coefficients involved in the above modeling formula are reported in Table I. Figure 4 illustrates the comparison of the calculated (dot lines) and simulated (solid lines) supply current. The coefficient of determination [37] is used to measure the correlation between model predicts f_i and actual data y_i, given as Equation (14).

$$R^2 = 1 - \frac{\sum_i (y_i - f_i)}{\sum_i (y_i - \hat{y})} \quad (14)$$

where $\hat{y}$ is the average value of actual data. A closer value of R^2 to 1means that the model-based predictions fit the actual data better. In Table II, we list R^2 values of modeling formula for various D-type FFs. As we can see from the table, the developed model is consistent with the simulation results, showing that our modeling formula can depict the actual data correctly.

TABLE I

FITTING COEFFICIENTS FOR CURRENT MODELING OF DFFHQX2

D-type FF	Transition Conditions			
	$0 \to 0$	$1 \to 1$	$1 \to 0$	$0 \to 1$
α_1	-12.0659	-5.6653	N/A	N/A
α_2	91.1392	73.6896	N/A	N/A
K	N/A	N/A	158.7772	495.8686
g	N/A	N/A	0.0450	0.0825
C_m	N/A	N/A	-22.9754	-5.1391
I_2	46.3265	48.9291	69.6209	74.7654
β_{11}	0.4628	0.4620	0.4672	0.4696
β_{12}	0.1227	0.1446	0.1679	0.1855
β_{21}	0.4565	0.4531	0.4456	0.4333
β_{22}	0.0145	0.0306	0.0991	0.1151
β_{p1}	N/A	N/A	N/A	0.4712
β_{p2}	N/A	N/A	N/A	0.1849
σ_1	0.0922	0.0831	0.0691	0.0604
γ_1	0.1214	0.1189	0.0918	0.0560
γ_2	-0.0109	-0.0005	0.0466	0.0750
λ_1	N/A	N/A	N/A	0.0028
λ_2	N/A	N/A	N/A	0.0106

N/A: Data not exist.

TABLE II

R^2 OF MODELING FORMULA

R^2	Transition Conditions			
	$0 \to 0$	$1 \to 1$	$1 \to 0$	$0 \to 1$
DFFHQX1	0.9499	0.9507	0.9604	0.9905
DFFHQX2	0.9405	0.9536	0.9353	0.9798
DFFHQX4	0.9415	0.9544	0.9079	0.9346
DFFRHQX1	0.8622	0.9163	0.9548	0.9347
DFFRHQX2	0.9318	0.9531	0.9400	0.9838
DFFRHQX4	0.9303	0.9522	0.8972	0.9860

C. Security Modeling for Clock Network

Simulated supply currents serve as the connection between state transitions and EM side-channel leakage. Based on the simulated supply currents, we can quantify the EM side-channel security for the clock network. We use the t-test statistic from TVLA technique as our security metric. A higher value of t-test statistic indicates a higher possibility that the design leaks sensitive data. Here we adopt the semifixed vs random t-test to avoid the false-positive result using the fixed data set [38]. During security modeling, we create the input stimuli for the semi-fixed dataset and random data set as described in [39]. Gate-level simulation is performed on the design to record the switching information of FFs in the value change dump (VCD) format. Under each stimulus,

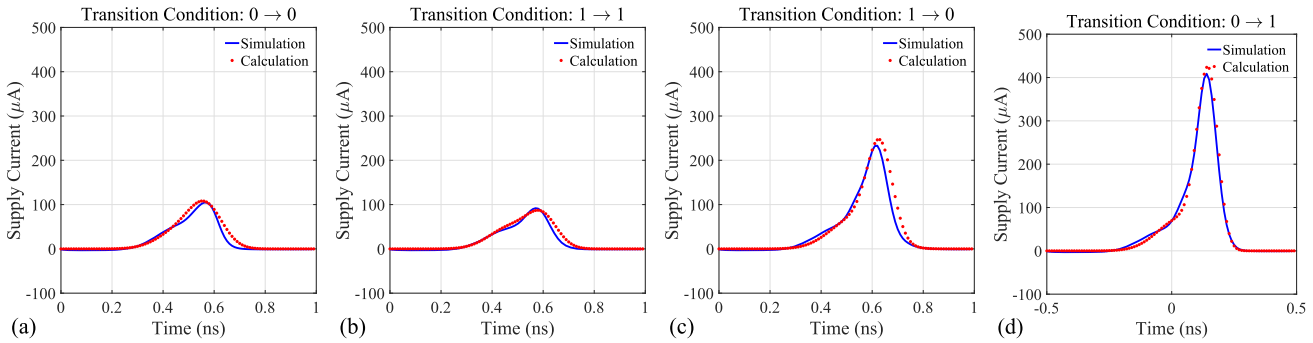

Fig. 4. The comparison of the calculated (dot lines) and simulated (solid lines) supply current of the FF under transition condition: (a) $0 \rightarrow 0$, (b) $1 \rightarrow 1$, (c) $1 \rightarrow 0$, and (d) $0 \rightarrow 1$.

the simulated supply current is represented by $\sum_{i \in all} I_{FF_i}^{TS_j}$ (Equation (6) to Equation (13)) which sums contributions of all FFs at j-th state transition. The time resolution during each state transition is set based on the trade-off between modeling accuracy and computational time. The clock network parameters involved in the above process, e.g., types, skew, slew and output load, are extracted from the physical design. Thereby we acquire the two data sets where one set Q_0 with n_0 semi-fixed stimuli another set Q_1 with n_1 random stimuli. According to Equation (15), we calculate the value t of t-test statistic which serves as the security metric for the clock network tunning.

$$t = \frac{E(Q_0) - E(Q_1)}{\sqrt{\frac{Var(Q_0)}{n_0} + \frac{Var(Q_1)}{n_1}}} \tag{15}$$

As mentioned in Section II-A, modern EDA tools pursue high performance by skew, slew and power reduction. This means that the side-channel leakage for different components has similar patterns and they aggregate in the time domain, leading to highly different values between the two sets. Hence a high t-test statistic increases the side-channel security risks. Based on the above observations, the extra uncertainties can be merged into temporary attributes of supply currents by configuring the clock skew, clock slew and load capacitance. Also, the amplitude attributes of the supply currents can be lowered by configuring the load capacitance and FFs' size. Along with security constraints, we can induce deviations on traces through tuning the clock signal distribution, and thus lead to a lower t-test value. Consequently, the EM side-channel leakage is adjusted to reduce the leaked information.

IV. CAD for EM Security Tools

The IC design flow illustrated in Figure 5 shows that the developed CAD4EM-CLK tool will be integrated into the flow between the *Clock Tree Synthesis* stage and the *Routing* stage. The inputs of the CAD4EM-CLK include the design netlist, a buffer list, a configuration file, performance constraints and security constraints.

The design netlist is the output of the current *Clock Tree Synthesis* and contains the clock network before applying security constraints. The buffer list is derived from the standard cell library. The security constraints are exerted in the form

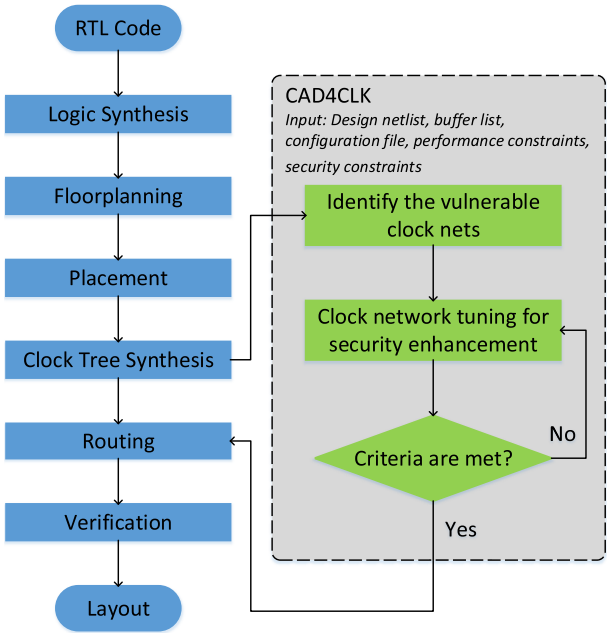

Fig. 5. The workflow of CAD4EM-CLK compatible with the existing design flow.

of the cost function, which models security quality for the clock network specified in Section III. The involved formula parameters in security constraints are represented by lookup tables.

The configuration file includes the user-defined settings for the execution of CAD4EM-CLK.

With these inputs, the CAD4EM-CLK tool will execute two main steps in balancing the security metric with other performance metrics. The tool first identifies the vulnerable nets of the initial clock network. It then reconfigures the clock network structure such as the level amount, buffer type, cluster amount, register order and size, in the vulnerable nets guided by the quantified security constraints. Due to the adjustment of the clock network, this protection will sacrifice the speed performance and thus be more suitable for these circuits often running at low frequencies.

A. Identify Vulnerable Clock Nets

During this step, CAD4EM-CLK extracts the total clock network from the design netlist. Through breadth-first search, every cell driven by the clock signal is sorted out and

represented in a tree-style graph. Each branch of the graph starts from the clock source, passes through the buffers group and ends with clock pins of corresponding FFs. The FFs that associate with the cryptographic operations are labeled as sensitive FFs to be protected. This can be realized by two ways. First, given the knowledge of the chip functionality, the designer knows the secure asset and provides a list of sensitive FFs, e.g., state FFs. Second, with the knowledge of the leakage model methods such as architecture correlation analysis (ACA) will be exploited to rank the FFs by calculating their contribution to the side-channel leakage [40]. Then the tool marks nets that connect to these FFs as the vulnerable clock nets V_{net}, including clock sources, buffers, FFs and their connectivity. Note that both signal-relevant and noise-relevant nets are treated by structure tunning, with the goal of reducing the information leakage.

B. Clock Network Tuning for Security Enhancement

This step will enhance the resistance of clock nets against EM side-channel attacks. Different from traditional PAS optimization processes, this optimization process is a balance among all PASS metrics, mainly a tradeoff among power, speed and security. This procedure is termed the combinatorial optimization problem and known to be NP-complete. For CAD4EM-CLK, we use the simulated annealing algorithm [41] to solve this problem. The overall flow is described in Algorithm 1.

In the initialization stage (Line 1 in Algorithm 1), the CAD4EM-CLK tool reads the user-defined parameters for simulated annealing by parsing the configuration file, including the start temperature $startTemp$, stop temperature $stopTemp$, cooling coefficient κ, maximum iteration of degradation optimization $maxItr$. The current temperature $currentTemp$ is set as $startTemp$. The iteration counter $currentItr$ is set as 0, denoting the number of iterations if the optimization process moves to the wrong direction. The current design $currentDsg$ is initialized as given design D, and its total power $initialPwr$ is obtained through power analysis. The user will also define the maximum power overhead $pwrCoeff$. For the vulnerable nets, the clock network structure $currentStruc$ is initialized as mentioned in section IV-A. Its security quality is determined by using function COSTFUNCTION (Line 34-37 in Algorithm 1). In this function, the tool extracts the following parameters from $currentDsg$, containing types, skew, slew and output load of every FFs for vulnerable clock nets. As analyzed in Section III-C, the tool will model supply currents and then quantify the security attributes by calculating the value of t-test statistic.

After initializing all settings, the subsequent iterations start to tune the clock structure (Line 2-23 in Algorithm 1). We define four factors to describe the structural features of the buffered clock tree. The cluster amount ϵ_1 determines the number of clock branch. The level amount ϵ_2 and buffer type ϵ_3 denote the number and type of buffers for insertion in each branch. The register order ϵ_4 and size ϵ_5 determine the connected register and its drive strength. Note

Algorithm 1 Clock Network Tuning for PASS Tradeoff

Input: Design netlist D, buffer list B, performance constraints (maximum power overhead $pwrCoeff$), security constraints and simulated annealing configuration file (start temperature $startTemp$, stop temperature $stopTemp$, cooling coefficient κ, maximum iteration of degradation optimization $maxItr$).
Output: Physical design with the secured clock network.

1 **Initial** $currentTemp \leftarrow startTemp$, $currentItr \leftarrow 0$, $currentStruc \leftarrow V_{net}$, $currentDsg \leftarrow D$, $InitialPwr \leftarrow$ *Power Analysis* on $currentDsg$, $currentScy \leftarrow$ COSTFUNCTION()
2 **repeat**
3 $judgeTime \leftarrow$ TIMECHECK()
4 **if** $judgeTime = 0$ **then**
5 break
6 **else**
7 **repeat**
8 $nextStruc \leftarrow random\{\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4, \epsilon_5 \in V_{net} \cup \mathbb{B}\}$
9 $currentDsg \leftarrow postCTS$ on design with $nextStruc$
10 $judgePwr \leftarrow$ PWRCHECK()
11 **until** $judgePwr = 1$;
12 $nextScy \leftarrow$ COSTFUNCTION()
13 $dE \leftarrow nextScy - currentScy$
14 $judgeScy \leftarrow$ SCYCHECK()
15 **if** $judgeScy = 1$ **then**
16 $currentStruc \leftarrow nextStruc$
17 $currentScy \leftarrow nextScy$
18 **if** $dE < 0$ **then**
19 $currentTemp \leftarrow currentTemp \times \kappa$
20 **else**
21 $currentItr \leftarrow currentItr + 1$
22 **until** $currentTemp \leq stopTemp$ *or* $currentItr \geq maxItr$;
23 **Function** `TimeCheck(`$currentDsg$`)`**:**
24 $timingRpt \leftarrow$ *Static Timing Analysis* on $currentDsg$
25 **if** $timingRpt$ *has violations* **then**
26 $judgeTime \leftarrow 0$
27 **else**
28 $judgeTime \leftarrow 1$
29 **return** $judgeTime$
30 **Function** `PwrCheck(`$currentDsg, initialPwr, pwrCoeff$`)`**:**
31 $pwrRpt \leftarrow$ *Power Analysis* on $currentDsg$
32 **if** $pwrRpt \leq initialPwr \times pwrCoeff$ **then**
33 $judgePwr \leftarrow 1$
34 **else**
35 $judgePwr \leftarrow 0$
36 **return** $judgePwr$
37 **Function** `CostFunction(`$currentDsg$`)`**:**
38 extract type, skew, slew, load from $currentDsg$
39 t-test calculation based on modeled supply currents
40 **return** t-test statistic
41 **Function** `ScyCheck(`$dE, currentTemp$`)`**:**
42 **if** $dE < 0$ **then**
43 $judgeScy \leftarrow 1$
44 **else if** $exp(-dE/currentTemp) > random(0, 1)$ **then**
45 $judgeScy \leftarrow 1$
46 **else**
47 $judgeScy \leftarrow 0$
48 **return** $judgeScy$

that cluster amount and level amount subject to performance constraints, such as maximum fanout and maximum latency. Therefore, the new clock structure $nextStruc$ can be adjusted by combining these randomly generated factors. In each iteration, CAD4EM-CLK generates a script that consists of multiple text commands, e.g., *addInst*, *addNet*, *attachTerm*, *ecoChangeCell*. These commands will guide the layout tool, e.g., Cadence Encounter [42], to implement a new clock network. Meanwhile, post-CTS optimizations are performed to solve problems including design rule violations, setup and hold violations and congestion reduction. The function TIMECHECK (Line 24-28 in Algorithm 1) is performed on updated design $currentDsg$ to check whether the optimization violates target speed constraints. If the design still has timing violations, the tool will report failure and exit. In addition, function PWRCHECK (Line 29-33 in Algorithm 1) is carried out to check whether the power consumption of $currentDsg$ exceeds the threshold. $pwrCoeff$ represents the allowed power overhead (more precisely, $initialPwr \times pwrCoeff$). If exceeds, the clock network will be retuned.

For each $nextStruc$ that passes the above checks, its security $nextScy$ is calculated and then evaluated by using function SCYCHECK (Line 38-43 in Algorithm 1). According to $nextScy$ and $currentTemp$, this function determines whether to accept $nextStruc$ as the current structure $currentStruc$ for next round iteration. If passed, the $currentScy$ is also updated. More specifically, the value of dE is negative showing that the optimization is close to the optimal solutions and we accept it directly. Otherwise, we accept the worse solutions with some temperature-dependent probabilities less than 1. Hence in Line 45, we select a random value that ranges from 0 to 1 as the threshold. This operation ensures that the algorithm would obtain the global optimum solution instead of the local optimum solution. The $currentTemp$ updates (multiplied by κ) only when $nextScy$ is less than $currentScy$. Otherwise, the $currentItr$ increases by 1. The above iterations continue until an exit criterion is fulfilled, i.e., the stop temperature or maximum iteration is achieved.

V. SIMULATION RESULTS FOR EM SIDE-CHANNEL PROTECTION

We will exploit layout-level EM simulation to validate the effectiveness of CAD4EM-CLK tool targeting on a 32-bit Substitution Box (SBox) in a 128-bit AES design.[3] This circuit consists of four 8-bit SBox modules and each module is implemented with the composite filed algorithm. In SCA attacks, SBoxes in cryptographic circuits are often the exploitation targets. An SBox takes in an input and uses the consecutive multiplicative inversions and affine transformation to derive the output. This relationship is well documented and central to many SCA attacks, especially correlational attacks. By comparing the correlation between recorded SBox operations and predicted values based on the known field transformation and keys for the same plaintexts, the key in use can be recovered [2], [31].

[3]Note that our method can be applied to the whole AES implementation but due to the very slow layout-level EM simulation process, we only demonstrate our method on an AES SBox [43]–[45].

TABLE III
CAD4EM-CLK PARAMETERS FOR THE EXPERIMENTS

$startTemp$	$stopTemp$	κ	$maxItr$	$pwrCoeff$
1×10^3	1×10^{-1}	0.7	1×10^4	1.2

A. CAD4EM-CLK Implementation

We first synthesize the RTL codes using SMIC 0.18-μm CMOS technology by Synopsys Design Compiler [46]. The synthesized netlist of the AES-SBox contains 908 gates with 32 DFFRHQ type FFs. Then we exploit the Cadence Encounter to place and route the design with the default core utilization setting of 70%. The chip area is 227μm $\times$ 226μm and four metal layers are occupied. We set the clock frequency and the supply voltage as 20MHz and 1.8V, respectively. The input data of the AES-SBox is obtained by XORing the key with plaintext. we assume the key is unknown while plaintexts are known. The adversary will recover the input data by CEMA attacks first and then infer the key.

In our experiment, the buffer list is of drive strength from X1 to X20 based on the technology library and the drive strength for FFs ranges from X1 to X4. Other parameters to configure CAD4EM-CLK tool are listed in Table III. The total clock tree security enhancement process using CAD4EM-CLK takes 26 minutes for the AES-SBox on a platform of an Intel 1.6GHz CPU with 8GB RAM.

B. EM Simulation and Security Analysis

To assess the EM side-channel resistance, we use the layout-level simulation method in [47], [48] to perform simulated CEMA attacks on the design. After various verifications, such as design rule checking (DRC) and layout versus schematic (LVS) checking, the design will go through layout-level parasitics extraction using the Calibre xRC. The inner parasitic resistance and capacitance are calculated and reported in the format of DSPF netlist. Note that we select the transistor-level type to get high-accuracy results in the parasitic extraction. Hspice is used to perform layout-level simulation on the circuit netlist annotated with parasitics and obtains transient currents per metal wire. By interpreting the parasitic netlist, we can obtain the actual location, width, length, and layer of each metal wire. Thereby using Maxwell equations and superposition principle, we calculate the EM emanations from the IC on the basis of obtained information of surface currents per metal wire, such as their amplitude, direction, location and size.

After collecting EM traces, we perform EM side-channel attacks on the AES-SBox design with and without the CAD4EM-CLK protection. Figure 6 presents the maximum correlations for all hypothetical key candidates. $\rho_{max} \approx 0.5216$ for unprotected AES-SBOX while $\rho_{max} \approx 0.2158$ for design with CAD4EM-CLK protection, reducing by 58.60%. In general, the maximum correlations of hypothetical keys will decrease gradually as increasing the number of traces N_{trace}, as shown in Figure 7. Starting from certain traces, the correlation for the correct hypothesis (red curve) will

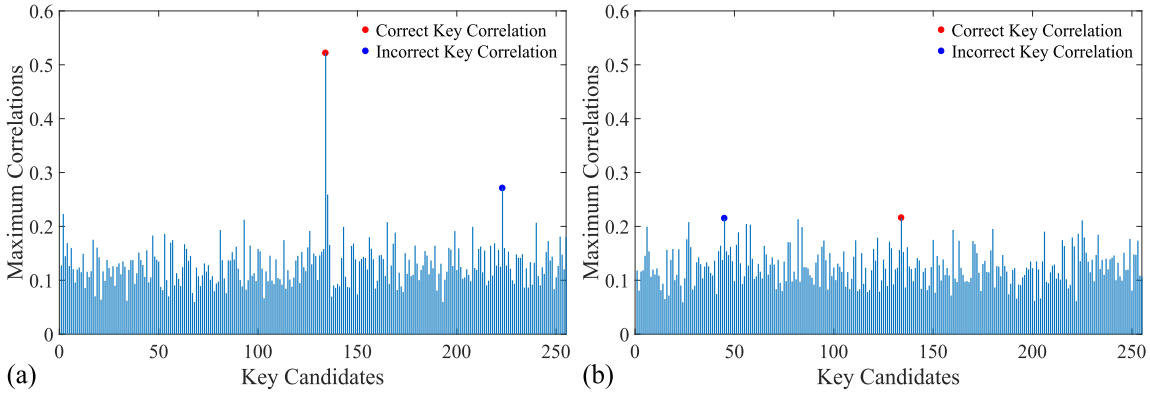

Fig. 6. CEMA attack results on the (a) AES-SBox without protection (b) AES-SBox with CAD4EM-CLK.

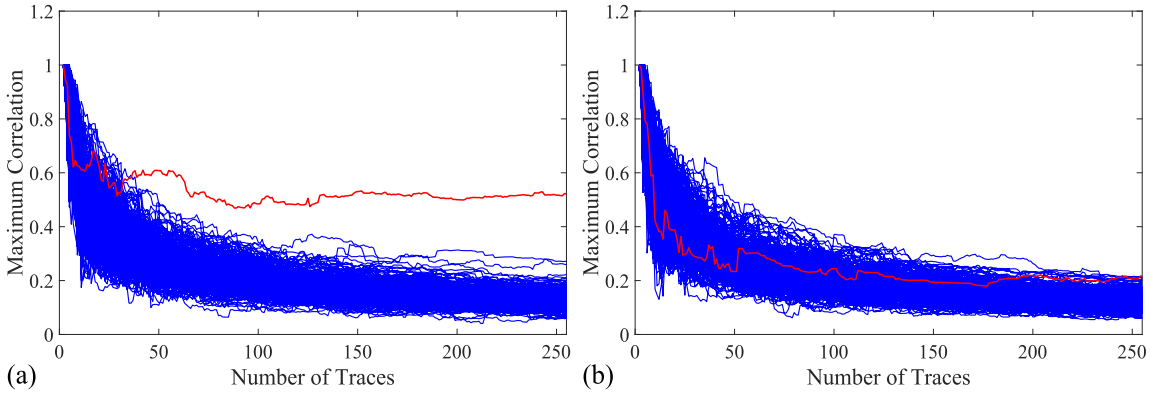

Fig. 7. CPA attack results on the (a) AES-SBox without protection (b) AES-SBox with CAD4EM-CLK.

TABLE IV
BALANCE OF SECURITY AND OVERHEADS FOR AES-SBOX DESIGN

AES-SBox	Without protection	With protection
Clock Latency (ns)	2.332	2.801
Clock Skew (ns)	0.0052	2.358
Clock Slew (ns)	0.126	0.182
Maximum Frequency (Mhz)	28	25
Total Area (μm^2)	51320	51320
Placement Density (%)	72.61	74.12
Total Power (mW)	0.4752	0.5135
Maximum Correlation	0.5216	0.2158
MTD	30	250

TABLE V
BALANCE OF SECURITY AND OVERHEADS FOR AES-128 DESIGN

AES-128	Without protection	With protection
Clock Latency (ns)	1.568	3.562
Clock Skew (ns)	0.049	2.77
Clock Slew (ns)	0.424	2.709
Maximum Frequency (Mhz)	45	35
Total Area (μm^2)	810000	810000
Placement Density (%)	60.66	61.82
Total Power (mW)	5.56	6.21
Maximum Correlation	0.5669	0.1521
MTD	48	552

always be above those with wrong hypotheses (blue curves). This minimum number of traces to disclosure (MTD) the key is denoted as N_{MTD}. After applying CAD4EM-CLK, the value of N_{MTD} increases from about 30 to about 250. This means that the resistance of AES-SBox against EM analysis attacks is improved by at least 8×.

In Table IV, we list the required overhead introduced by the proposed tool targeting on AES-SBox design, including timing, area and power overheads. In terms of timing overheads, for the AES-SBox using current design flow, the clock latency τ_l, the clock skew τ_a and the clock slew τ_s are 2.332ns, 0.0052ns and 0.182ns, respectively. After applying CAD4EM-CLK, the above objectives have changed due to tuned clock network, where $\tau_l = 2.801$ns, $\tau_a = 2.358$ns and $\tau_s = 0.182$ns. Note that these alterations do not introduce any timing violations. But the maximum frequency changes from 28 Mhz to 25 Mhz after applying the tool on AES-SBox design. In terms of area overheads, the total area remains unchanged while the placement density slightly increases from 72.61% to 74.12%. In terms of power overheads, the total power changes from $P_{total} = 0.4752$mW before the security enhancement to $P_{total} = 0.5135$mW after the security enhancement, an increase by 8.06%. The increase is well below the defined threshold of 20% (users can specify other thresholds). Therefore, it can be found that the CAD4EM-CLK tool balances the whole design requirements of PASS metrics.

VI. SIMULATION RESULTS FOR POWER SIDE-CHANNEL PROTECTION

As we mentioned earlier, CAD4EM-CLK is also suitable for protecting the power side channels, in addition to the EM side-channel. In this section, we will validate its extensibility

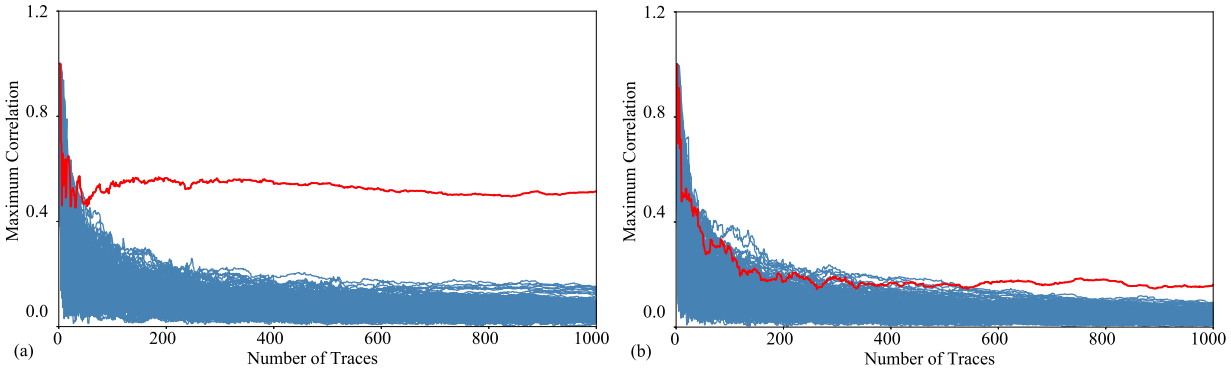

Fig. 8. CEMA attack results on the (a) AES-128 without protection (b) AES-128 with CAD4EM-CLK.

through layout-level power simulation on a complete 128-bit AES design.

A. CAD4EM-CLK Implementation

The complete 128-bit AES design [49], denoted as AES-128, has ten rounds of encryptions after the KeySchedule operation. One round of encryption executes four operations including SubBytes, ShiftRows, Mixcolumns (except the last round) and AddRoundKey. Moreover, each round encryption occupies five clock cycles where the first four are assigned for S-Boxes and the last for other operations. Intermediate data and final output data from these operations are stored and transmitted using state registers. The AES-128 design first passes RTL-to-GDS to create a physical layout. The final layout contains 12063 gates with 1892 FFs, and occupies 900μm $\times$ 900μm die area. Other physical parameters of AES-128 and the CAD4EM-CLK tool are the same as mentioned in Section V-A.

B. Power Simulation and Security Analysis

We leverage the PrimeTime PX tool to carry out time-based power simulations on physical design. This tool will build a detailed power profile of the design based on the layout-level netlist, design constraints, parasitics and Value Change Dump (VCD) for specified switching activity. Then Correlational Power Analysis (CPA) attacks are performed on the collected power traces for security evaluation. Figure 8 illustrates the attack results that the evolution of the hypothetical keys' correlations with increased power traces. As shown in Figure 8(a) $N_{MTD} \approx 48$ and $\rho_{max} \approx 0.5669$ for AES-128 without protection. After applying CAD4EM-CLK, $\rho_{max} \approx 0.1521$ and $N_{MTD} \approx 552$ showing that the proposed tool boost the security by at least $11\times$.

The overhead of the CAD4EM-CLK tool for protecting AES-128 is listed in Table V. In terms of timing overheads, comparing the design AES-128 before and after protection, the clock latency τ_l, the clock skew τ_a and the clock slew τ_s grow from 1.568ns, 0.049ns and 0.424ns to 3.562ns, 2.77ns and 2.709ns, respectively. Correspondingly, the maximum frequency changes from 45 Mhz to 35 Mhz after protection. In terms of area overheads, the total area remains unchanged while the placement density slightly increases from 60.66% to 61.82%. In terms of power overheads, the total power $P_{total} = 5.56$mW before the security enhancement and $P_{total} = 6.21$mW after the security enhancement, an increase by 11.70%.

VII. Conclusion

In this paper, we propose a CAD for Security tool, named CAD4EM-CLK, to incorporate security constraints into modern EDA tools, while also maintaining other performance constraints like power, area and speed. Guiding by all PASS metrics, the tool can tune the clock network automatically to enhance power and EM side channel resistance while still meeting all other constraints. Utilizing layout-level EM simulation, we carry out CEMA attacks on the AES-SBox protected by CAD4EM-CLK. Additionally, we validate the effects of CAD4EM-CLK on a simulated power SCA attack targeting a complete AES design. Experimental results validate that the tool can achieve a tradeoff among all PASS metrics. In the future, we will try to integrate the developed CAD for Security tool into the open-source EDA toolchain. Also, we will optimize the tool to introduce dynamic randomization to further enhance the CAD4EM-CLK tool.

References

[1] 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)*, Oct. 2015, pp. 296–303.

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

[3] Y. Jin and Y. Makris, "Hardware Trojan detection using path delay fingerprint," in *Proc. IEEE Int. Workshop Hardware-Oriented Secur. Trust (HOST)*, Jun. 2008, pp. 51–57.

[4] J. Danial, D. Das, S. Ghosh, A. Raychowdhury, and S. Sen, "SCNIFFER: Low-cost, automated, efficient electromagnetic side-channel sniffing," *IEEE Access*, vol. 8, pp. 173414–173427, 2020.

[5] A. Gornik, A. Moradi, J. Oehm, and C. Paar, "A hardware-based countermeasure to reduce side-channel leakage: Design, implementation, and evaluation," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 34, no. 8, pp. 1308–1319, Aug. 2015.

[6] P. Maistri, S. Tiran, P. Maurine, I. Koren, and R. Leveugle, "Countermeasures against EM analysis for a secured FPGA-based AES implementation," in *Proc. Int. Conf. Reconfigurable Comput. FPGAs (ReConFig)*, Dec. 2013, pp. 1–6.

[7] A. Dubey, R. Cammarota, and A. Aysu, "MaskedNet: The first hardware inference engine aiming power side-channel protection," in *Proc. IEEE Int. Symp. Hardw. Oriented Secur. Trust (HOST)*, Dec. 2020, pp. 197–208.

[8] A. Dubey, R. Cammarota, and A. Aysu, "BoMaNet: Boolean masking of an entire neural network," in *Proc. 39th Int. Conf. Comput.-Aided Design (ICCAD)*, Nov. 2020, pp. 1–9.
[9] G. Li, V. Iyer, and M. Orshansky, "Securing AES against localized EM attacks through spatial randomization of dataflow," in *Proc. IEEE Int. Symp. Hardw. Oriented Secur. Trust (HOST)*, May 2019, pp. 191–197.
[10] 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.
[11] M. Arsath K F, V. Ganesan, R. Bodduna, and C. Rebeiro, "PARAM: A microprocessor hardened for power side-channel attack resistance," in *Proc. IEEE Int. Symp. Hardw. Oriented Secur. Trust (HOST)*, Dec. 2020, pp. 23–34.
[12] C. Wang, Y. Cai, H. Wang, and Q. Zhou, "Electromagnetic equalizer: An active countermeasure against EM side-channel attack," in *Proc. Int. Conf. Comput.-Aided Design*, Nov. 2018, p. 112.
[13] D. Das, M. Nath, B. Chatterjee, S. Ghosh, and S. Sen, "STELLAR: A generic EM side-channel attack protection through ground-up root-cause analysis," in *Proc. IEEE Int. Symp. Hardw. Oriented Secur. Trust (HOST)*, May 2019, pp. 11–20.
[14] D. Das *et al.*, "EM and power SCA-resilient AES-256 through $>350\times$ current-domain signature attenuation and local lower metal routing," *IEEE J. Solid-State Circuits*, vol. 56, no. 1, pp. 136–150, Jan. 2021.
[15] T. Ikematsu, Y.-I. Hayashi, T. Mizuki, N. Homma, T. Aoki, and H. Sone, "Suppression of information leakage from electronic devices based on SNR," in *Proc. IEEE Int. Symp. Electromagn. Compat.*, Aug. 2011, pp. 920–924.
[16] M. Kar *et al.*, "Blindsight: Blinding EM side-channel leakage using built-in fully integrated inductive voltage regulator," 2018, *arXiv:1802.09096*. [Online]. Available: http://arxiv.org/abs/1802.09096
[17] 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.
[18] Y.-Y. Chen, C. Dong, and D. Chen, "Clock tree synthesis under aggressive buffer insertion," in *Proc. 47th Design Autom. Conf. (DAC)*, 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] C. Sitik, W. Liu, B. Taskin, and E. Salman, "Low voltage clock tree synthesis with local gate clusters," in *Proc. Great Lakes Symp. VLSI*, May 2019, pp. 99–104.
[21] 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.*, Jun. 2016, p. 82.
[22] K. Tiri and I. Verbauwhede, "A VLSI design flow for secure side-channel attack resistant ICs," in *Proc. Design, Automat. Test Eur.*, Munich, Germany, 2005, pp. 58–63.
[23] S. Guilley, F. Flament, P. Hoogvorst, R. Pacalet, and Y. Mathieu, "Secured CAD back-end flow for power-analysis-resistant cryptoprocessors," *IEEE Des. Test. Comput.*, vol. 24, no. 6, pp. 546–555, Nov. 2007.
[24] A. G. Bayrak, N. Velickovic, F. Regazzoni, D. Novo, P. Brisk, and P. Ienne, "An EDA-friendly protection scheme against side-channel attacks," in *Proc. Design, Autom. Test Eur. Conf. Exhib. (DATE)*, 2013, pp. 410–415.
[25] S. Huss and O. Stein, "A novel design flow for a security-driven synthesis of side-channel hardened cryptographic modules," *J. Low Power Electron. Appl.*, vol. 7, no. 1, p. 4, Feb. 2017.
[26] P. Slpsk, P. K. Vairam, C. Rebeiro, and V. Kamakoti, "Karna: A gate-sizing based security aware EDA flow for improved power side-channel attack protection," in *Proc. IEEE/ACM Int. Conf. Comput.-Aided Design (ICCAD)*, Nov. 2019, pp. 1–8.
[27] J.-J. Quisquater and D. Samyde, "ElectroMagnetic analysis (EMA): Measures and counter-measures for smart cards," in *Proc. Int. Conf. Res. Smart Cards*. Berlin, Germany: Springer, 2001, pp. 200–210.
[28] J.-L. Lacoume, "A proposition for correlation power analysis enhancement," in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst.* Berlin, Germany: Springer, 2006, pp. 174–186.
[29] B. Gierlichs, L. Batina, P. Tuyls, and B. Preneel, "Mutual information analysis," in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst.* Berlin, Germany: Springer, 2008, pp. 426–442.
[30] T. Schneider and A. Moradi, "Leakage assessment methodology," in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst.* Berlin, Germany: Springer, 2015, pp. 495–513.
[31] J. He, H. Ma, X. Guo, Y. Zhao, and Y. Jin, "Design for EM side-channel security through quantitative assessment of RTL implementations," in *Proc. 25th Asia South Pacific Design Autom. Conf. (ASP-DAC)*, Jan. 2020, pp. 62–67.
[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] H. Ma, J. He, Y. Liu, Y. Zhao, and Y. Jin, "CAD4EM-P: Security-driven placement tools for electromagnetic side channel protection," in *Proc. Asian Hardw. Oriented Secur. Trust Symp. (AsianHOST)*, Dec. 2019, pp. 1–6.
[34] 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.
[35] C. J. Alpert, D. P. Mehta, and S. S. Sapatnekar, *Handbook of Algorithms for Physical Design Automation*. Boca Raton, FL, USA: Auerbach, 2008.
[36] 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 *Proc. Int. Conf. Smart Card Res. Adv. Appl.* Berlin, Germany: Springer, 2012, pp. 248–262.
[37] D. Zhang, "A coefficient of determination for generalized linear models," *Amer. Statistician*, vol. 71, no. 4, pp. 310–316, Oct. 2017.
[38] G. Becker *et al.*, "Test vector leakage assessment (TVLA) derived test requirements (DTR) with AES," in *Proc. Int. Cryptograph. Module Conf.*, 2013, pp. 1–8.
[39] J. Cooper *et al.*, "Test vector leakage assessment (TVLA) methodology in practice," in *Proc. Int. Cryptograph. Module Conf.*, vol. 20, 2013, pp. 1–13.
[40] Y. Yao, T. Kathuria, B. Ege, and P. Schaumont, "Architecture correlation analysis (ACA): Identifying the source of side-channel leakage at gate-level," in *Proc. IEEE Int. Symp. Hardw. Oriented Secur. Trust (HOST)*, Dec. 2020, pp. 188–196.
[41] R. H. Otten and L. P. van Ginneken, *The Annealing Algorithm* (The Kluwer International Series in Engineering and Computer Science), vol. 72. Boston, MA, USA: Springer, 1989.
[42] Cadence. *SOC Encounter*. Accessed: Nov. 20, 2020. [Online]. Available: https://www.cadence.com
[43] 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. (DAC)*, 2013, p. 78.
[44] F. Zhang, B. Yang, B. Yang, Y. Zhang, S. Bhasin, and K. Ren, "Fluctuating power logic: SCA protection by V_{DD} randomization at the cell-level," in *Proc. Asian Hardw. Oriented Secur. Trust Symp. (AsianHOST)*, 2019, pp. 1–6.
[45] M. M. Sharifi *et al.*, "A novel TIGFET-based DFF design for improved resilience to power side-channel attacks," in *Proc. Design, Autom. Test Eur. Conf. Exhib. (DATE)*, Mar. 2020, pp. 1253–1258.
[46] Synopsys. *Design Compiler*. Accessed: Nov. 20, 2020. [Online]. Available: https://www.synopsys.com
[47] 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.
[48] H. Ma, J. He, Y. Liu, L. Liu, Y. Zhao, and Y. Jin, "Security-driven placement and routing tools for electromagnetic side channel protection," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, early access, Sep. 21, 2020, doi: 10.1109/TCAD.2020.3024938.
[49] Secwork. (2014). *NIST Document FIPS 197 Based AES Design*. [Online]. Available: https://github.com/secworks/aes

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 (UCF) and the University of Florida (UF) from 2016 to 2018. He is currently a Post-Doctoral Research Fellow with the Institute of Microelectronics, Tsinghua University. His research interests include digital circuit design, hardware security, and EDA for security.

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

Yier Jin (Senior Member, IEEE) received the B.S. and M.S. degrees in electrical engineering from Zhejiang University, China, in 2005 and 2007, respectively, and the Ph.D. degree in electrical engineering from Yale University in 2012. He is currently an Associate Professor and a Warren B. Nelms IoT Term Professor with the Department of Electrical and Computer Engineering (ECE), University of Florida (UF). His research interests include hardware security, embedded systems design and security, trusted hardware intellectual property (IP) cores, and hardware-software co-design for modern computing systems. He is also interested in the security analysis on the Internet of Things (IoT) and wearable devices with particular emphasis on information integrity and privacy protection in the IoT era. He is the IEEE Council on Electronic Design Automation (CEDA) Distinguished Lecturer. He was a recipient of the DoE Early CAREER Award in 2016, the ONR Young Investigator Award in 2019, and the Best Paper Award from DAC'15, ASP-DAC'16, HOST'17, ACM TODAES'18, GLSVLSI'18, DATE'19, and AsianHOST'20.

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.