EMSIM+: Accelerating Electromagnetic Security Evaluation with Generative Adversarial Network

Ya Gao*‡, Haocheng Ma*‡, Jindi Kong*, Jiaji He*§, Yiqiang Zhao*, and Yier Jin†
*School of Microelectronics, Tianjin University
†University of Science and Technology of China
{gaoyaya, hc_ma, kongjindi, dochejj, yq_zhao}@tju.edu.cn, yier.jin@ustc.edu.cn

***Abstract*—Electromagnetic side-channel analysis (EM SCA) attack is a serious threat to integrated circuits (ICs). In order to detect vulnerabilities in time at the pre-silicon stage and to improve the chip's robustness to EM SCA attacks, several EM simulation methods have emerged for EM side-channel leakage evaluation. Although the simulated results are accurate, the chip security evaluation in practice requires up to hundreds of millions simulation traces, which imposes an unrealistic computational and time overhead on these simulator-based methods.**

In this paper, we develop a tool named EMSIM+. Different from the general EM security evaluation process, EMSIM+ introduces machine learning (ML) to accelerate the simulation of layout-level EM emanations. Based on the generative adversarial network (GAN), a well-trained EMSIM+ model can accept the cell current and power grid information of the chip and rapidly predict the EM emanation of the chip surface. We apply EMSIM+ to a series of representative cryptographic circuits and compare the simulation results with the state-of-the-art EM simulation method and silicon measurements. The experimental results prove that EMSIM+ has high simulation accuracy and achieves more than 242 times evaluation time reduction for 1 M sample data.

***Index Terms*—CAD for Security, Side-Channel Analysis, Generative Adversarial Network**

I. INTRODUCTION

Side-channel analysis (SCA) attack has long been a threat to the information security and functional security of integrated circuits (ICs) [1]. By collecting information such as electromagnetic (EM), power, and timing inadvertently released by devices, SCA attack can steal information such as the key of a cryptographic chip or the parameters of a neural network (NN) model [2]. Given the above risks, it is often necessary to evaluate the side-channel security of the chip before it is put into use. However, security evaluation is only performed after the chip is manufactured in common industrial practice. Once a chip does not meet security standards, industry faces high cost and time penalties incurred in redoing the entire design cycle. As a result, it is highly desirable to consider side-channel security evaluation prior to delivering the physical design to the foundry, i.e., the pre-silicon stage, which will enhance the flexibility to fix the design [3].

Among various side-channel information, EM emanations originate from the current inside IC components and contains a wealth of information in the spatial, temporal and frequency domains. Therefore, the EM SCA attack is considered as one of the most threatening means of SCA attacks [4], [5]. In order to perform EM security evaluation at the pre-silicon stage, EM simulation at layout level is fast emerging as an attractive option. By simulating an accurate EM map corresponding to the chip layout, side-channel security vulnerabilities can be quickly located in conjunction with SCA.

The topic of EM simulation for side-channel security evaluation has been explored in several papers. Li et al. construct a global EM information simulation flow for predicting information leakage from different processors in the design phase for the first time, involving current flow simulation, chip layout parasitic extraction and EM emanation calculation [6]. Nevertheless, the rapid growth in circuit size is also accompanied by a rapid growth in the size of the extracted parasitic network. Meanwhile, the complexity of simulating device models also grows exponentially, resulting in the simulation time explosion. Further, various methods to simplify EM simulation have been developed one after another. Lomne et al. establish a simulation process at the layout-level. They exploit Ansys RedHawk to simulate the transient currents of power and ground networks for EM calculations and obtain satisfactory results in terms of spatial and time resolutions [7]. To further accelerate the simulation flow, Kumar et al. perform a multiple-abstraction-level circuit analysis to identify current branches of critical cryptographic operations, with the help of the parallel mechanism of Synopsys FineSim [8]. Among the latest advances in EM simulation, Ma et al. address the tool namely EMSim, which reduces the computational complexities of layout-level EM simulations with parasitic network reduction and device model approximation [9]. Compared to traditional EM simulation methods, EMSim achieves a 32 times increase in efficiency and assists in locating EM leakage areas while maintaining high accuracy.

The above methods are effective in balancing the efficiency and accuracy of EM simulation, while assisting chip designers to avoid the risk of side-channel leakage in a timely manner. However, during evaluation, these methods all rely on simulators to solve large-scale systems of nonlinear equations to collect EM data. In security evaluation scenarios for high-security level chips, the demand often extends to millions or even hundreds of millions of EM traces [10]. As circuit complexity and data volume increase, even EMSim tool need to bear years of simulation overhead. Therefore, there is an urgent need for further accelerate the EM side-channel secu-

‡These authors contributed equally to this work.
§Corresponding author.

rity evaluation method to solve the bottleneck of insufficient scalability of the existing methods.

To optimize the pre-silicon EM evaluation process, we propose a generative adversarial network (GAN) based optimization method for EM side-channel security evaluation called EMSIM+[1]. GAN has the capacity to generate new data with additional information from the original data and is widely used for data prediction. This data prediction capability can effectively assist in generating EM evaluation samples. Figure 1 shows the difference between general flow and EMSIM+ flow. In general flow, EM emanations used for evaluation are obtained by general method. General method means traditional EM simulation tools such as EMSim or silicon measurements. In EMSIM+, a small set of sample pairs from cell currents, power grids to EM traces are simulated or collected by general method and then used as real data to train the model. Finally, the trained EMSIM+ model accurately and rapidly generates all the data needed for security evaluation, which greatly accelerates the security evaluation.

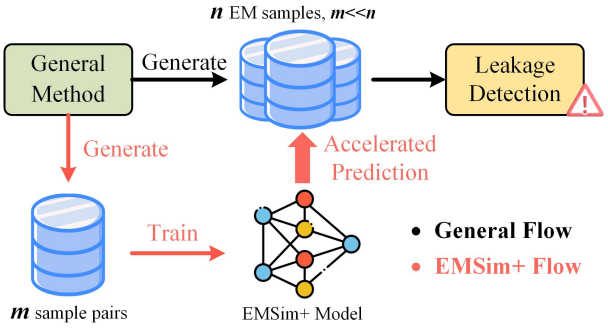


Fig. 1: General method vs. EMSIM+ flow.

The main contributions of this paper are highlighted as follows.

- We establish a fast GAN-based EM side-channel security evaluation tool named EMSIM+. It introduces ML to the EM security evaluation domain for the first time, allowing security-oriented evaluation and design more efficiently.
- EMSIM+ uses well-engineered feature maps extracted from the layout-level, which capture information about the cell current and power grid that cause the source of EM emanation. By using continuous time as one of the conditions, EMSIM+ learns the EM variations in dynamic time through an image-to-image translation manner.
- We apply EMSIM+ to a representative set of cryptographic circuits and compared the results with the latest EM simulation method, EMSim and the silicon-level measurements. The experimental results demonstrate that EMSIM+ has high simulation accuracy, and achieves 242 times evaluation time reduction for 1M sample data compared to EMSim.

The rest of this paper is organized as follows. Section II introduces the background about ML for electronic design automation (EDA) and the GAN family. Then, the details of our proposed EMSIM+ are shown in Section III. Section V and Section IV demonstrate the effectiveness of EMSIM+ on EM security evaluation. Conclusions are drawn in Section VI.

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

II. BACKGROUND

A. ML-based Electronic Design Automation (EDA)

Due to the rapid evolution of semiconductor technology, the exponential growth of ICs is putting forth greater demands on circuit performance and security. Traditionally, EDA or computer-aided design (CAD) tools rely on rule-based and deterministic algorithms to solve these complex tasks. However, the design and verification phases of ICs are becoming increasingly challenging with traditional methods alone as ICs complexity rises and the need for faster design cycles. In recent years, by harnessing the power of data-driven models, ML provides a fast and high-quality solution to the above challenges. ML algorithms facilitate the extraction of valuable insights from large datasets and aid in developing both accurate and efficient predictive models.

Currently, the use of ML to optimize EDA tools covers almost all stages of ICs' design and achieves prediction results that are comparable to those of traditional tools. Alawieh et al. translate placement schemes and the connectivity information as input images to speed up forecasting routing congestion map for large-scale FPGA via a conditional generative adversarial network (CGAN) [11]. Lu et al. propose a framework named GAN-CTS to solve clock tree synthesis (CTS) outcomes prediction and optimization problems by extracting features from trail routing, flip flops and clock net [12]. Chhabria et al. utilize an encoder-decoder based CGAN to perform thermal analysis and IR drop prediction based on potential characteristics of power distribution and density [13].

The above ML-based analysis methods substitute the multistep, high-complexity solution process and demonstrate an impressive ability to improve the efficiency of each subtask, even surpassing traditional methods. By training ML algorithms to learn from data and optimize computational processes, designers can drastically reduce the time and effort required to design and verify ICs systems, promoting more efficient and cost-effective designs.

B. Generative Adversarial Network (GAN) Family

GAN is a class of unsupervised ML generative models, initially developed by Goodfellow et al. in 2014 [14], as depicted in Figure 2. GAN unites two competing networks, a generator G and a discriminator D, to generate high-quality fake samples through an adversarial training process. More concretely, G generates predicted data $G(z)$ from a given noise input z. D is used to distinguish the real data x from the real-looking $G(z)$. A mainstream G basically use an encoder-decoder scheme, where the input is downsampled by convolution layers in the encoder until a bottleneck layer. Then this process is reversed by transpose convolution layers in the decoder. D takes the form of a convolutional neural network that performs similar functions to binary image classification.

During the training process, the competition in the game drives both G and D to improve their skills and eventually reach a Nash equilibrium. The final loss function is expressed as:

$$\min_G \max_D V(D,G) = E_{x\sim P_{\text{data}}(x)}[\log D(x)] + E_{z\sim P_z(z)}[\log(1-D(G(z)))] \quad (1)$$

where P_{data} represents the real data distribution and P_z represents the prior distribution for a given noise x.

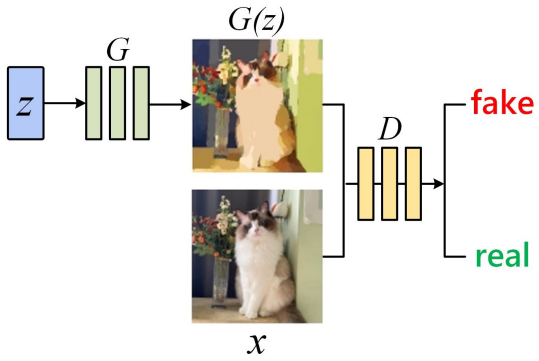


Fig. 2: The structure of a generative adversarial network.

With the increase of application scenarios, a series of models such as Conditional GAN (CGAN), Deep Convolution GAN (DCGAN), Wasserstein GAN (WGAN), etc. have been proposed to expand the GAN family. In the field of EM simulation, our goal is to reconstruct EM information based on current and power supply information through GAN. Therefore, the CGAN model, given its capacity for additional sample inputs, is particularly suitable for this task, allowing for the generation of more precise samples.

III. GAN BASED EMSIM+ FAMEWORK

The overview of the proposed GAN-based EMSIM+ is shown in Figure 3, including training phase, prediction phase and evaluation phase. During the training phase, we aim to design and train a GAN for EM prediction. Specifically, the generator G accepts three types of input features extracted from the circuit, i.e., cell current maps, power grid maps and time sequence. Then, both the EM maps predicted by G and the real EM maps, together with the input maps of G, are alternatively fed to the discriminator D for determination. The determination results are further fed back to G to enhance the quality of the predicted EM maps. During the prediction phase, G is preserved and serves as an inference model for EM prediction. The model can take the cell current maps and power gird map of any circuit as input and predict the EM maps that vary over a specific time sequence. Eventually, the evaluation phase gives feedback on whether the circuit has the risk of EM side-channel leakage. Here we focus on the training phase.

A. Feature Extraction

Based on the theoretical model of EM emanation from ICs in [9], the transient current data of logic cells and the topmost power grid are the sources of EM emanation. Therefore, we first extract the cell current and power grid information from the database of the chip physical layout, and convert them into feature maps, which are then combined as input features to G. Next, EM data is extracted by general EM simulation or measurement methods and mapped as real EM maps. Take a chip with a size of $w \times h$ as an example, its surface is divided into a matrix of grid tiles using a $l \times l$ square and represented as a feature map with a dimension of $m \times n$ pixels, i.e., $m = w/l$, $n = h/l$. EMSIM+ provides the ability for the user to select the granularity of the EM simulation themselves by adjusting l for any size chip.

1) cell current map: This feature contains the position coordinates of each logic cell and the transient current I_i, $i = 1, 2, ...n$, and n indicates the total number of logic cells of the chip. As illustrated in Figure 4, space decomposition divides cell current into any grid tiles (blue squares) occupied by the cells (gray rectangles). Assuming a uniform distribution of the current within grid tiles, the equivalent current of each grid tile is equal to the sum of all internal logic cells' current. For cells that cover more than one grid tile, we consider that it only contributes to the leftmost grid tile. Therefore, the equivalent current of the middle grid tile in Figure 4 is $I_2 + I_3 + I_5 + I_7$. The cell current map of size $m \times n \times t$ pixels is obtained by traversing all logical cells and adding the transient current to the corresponding grid tiles, where t is the length of the time sequence.

2) power grid map: This feature is generated by extracting the location coordinates of the power pad as well as the power supply metal wire. To express the equivalent resistance d of a single supply path, we measure the Manhattan distance from the center coordinates of the grid tile with a power supply metal wire (x_1, y_1) to the center of a power pad in x- and y-coordinates (x_2, y_2):

$$d = |x_1 - x_2| + |y_1 - y_2| \quad (2)$$

If power supply metal wires in a grid tile are connected to N power pads, the equivalent resistance d_e is calculated according to Equation 3.

$$d_e^{-1} = d_1 + d_2 + \ldots + d_N + C \quad (3)$$

The constant term C is used to avoid the anomaly that the denominator is zero. We iterate this procedure for all grid tiles and complete the power grid map of size $m \times n \times 1$ pixels. Intuitively, the density of the power network is also reflected in the feature map.

3) real EM map: This feature reflects the EM distribution over a specified height and time period. We produce real EM maps of size $m \times n \times t$ pixels for guiding EMSIM+ to generate high-precision EM maps.

B. GAN Architecture Design

We select a model named *pix2pix* from the CGAN category to convert the EM simulation of the chip into a paired image translation problem. At the top level, it consists of a *U-Net-based* generator and a *PatchGAN-based* discriminator.

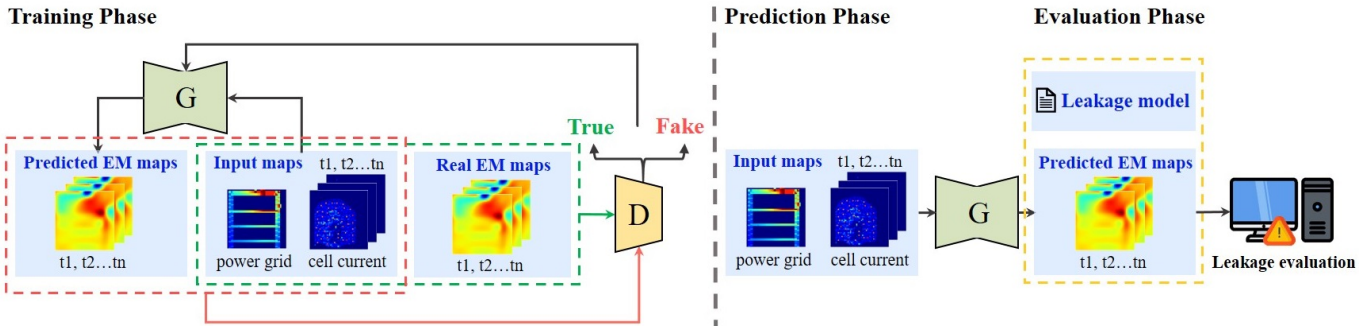


Fig. 3: The proposed GAN-based EMSIM+ framework.

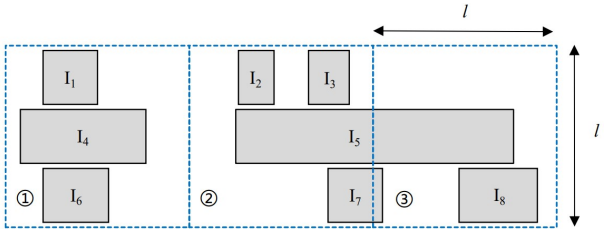


Fig. 4: Space decomposition of cell currents.

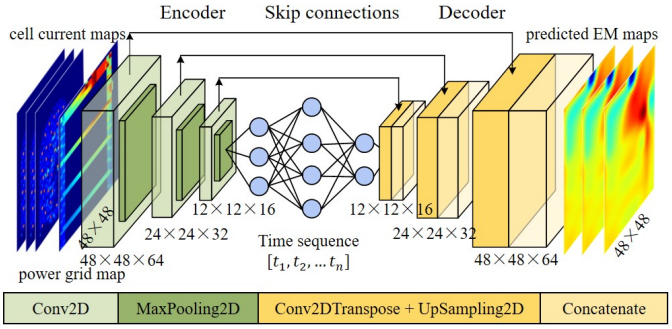


Fig. 5: The generator network of EMSIM+.

1) U-Net-based generator: In the context of EM prediction, the generator's role is to extract the features from the cell current maps frame-by-frame and a power grid map before converting them back to EM maps for all time steps. The details of the generator's structure are depicted in Figure 5. Specifically, the encoder comprises convolutional layers paired with max pooling layers that capture the essential high-dimensional features of the cell current maps and power grid map. The convolutional layer leverages varying numbers and sizes of kernels within the sliding window to extract local features of the input, using ReLU as the activation function. The max pooling layer subsequently condenses the dimensionality of these features by half. After down sampling operations, the encoder obtains effective features in low dimensions. The subsequent fully connected layer flattens the spatial features extracted by the encoder and fuses them with the time sequence.

The decoder is created by transpose convolutional and upsampling layers. By extending the dimension and depth of the feature matrix, the decoder can restore fine-grained information lost during the downsampling phase. A standard solution is to use skip connections to fully guarantee the comprehensive incorporation of the input information into output information and predict the realistic EM maps. Skip connections stack intermediate feature maps in the encoder directly to the corresponding layers in the decoder through concatenate layers, realizing the combination of global, temporal and location information. In this way, U-Net can accurately describe the spatial EM distribution while alleviating the gradient vanishing problem.

2) PatchGAN-based discriminator: The discriminator is implemented by the PatchGAN structure as an image classifier to determine whether input EM maps are real or not. PatchGAN divides the input map into multiple fixed-size grid tiles and calculates the probability of each grid tile being true individually. The average value of each grid tile is then used as the output of the discriminator to assist the generator in obtaining a higher quality EM map. It is important to note that the discriminator contains considerably fewer parameters than the generator. This is due to the fact that it solely depends on the deep network for consistent abstraction and generalization.

C. Model Training

To increase the scalability of EMSIM+, the parameters of our model are made adjustable and optional. The pixel dimensions of input feature maps, simulation time points, filter size, and even the dataset division can be adjusted to cater to various situations. As a proof of concept, we consider input and output feature maps with dimensions of 48×48 pixels, with hyperparameters used for model training are tabulated in Table I. The analysis period is assumed to be 20 ns, represented as a time sequence of 20. Before the training process, the dataset is split into 90% for training and 10% for validation, respectively. The training dataset is normalized to a range between 0 and 1. The EMSIM+ model applies the Adam optimizer during the training process, and the learning rate decays exponentially from 0.0005 with the discount factor 0.98. We choose Mean Squared Error (MSE) and Mean Absolute Error (MAE) for loss functions to yield the most effective performance. The entire model is constructed and tested in TensorFlow2.4. Both training and testing are

TABLE I: Hyperparameters of EMSIM+

Hyperparameter			Encoder	Decoder
Model layer parameters	Conv2D	filter size	3×3	7×7
	Conv2DTranspose	filter number	64	16
	Conv2D	filter size	3×3	7×7
	Conv2DTranspose	filter number	32	32
	Conv2D	filter size	3×3	3×3
	Conv2DTranspose	filter number	16	64
	Conv2D	filter size	–	3×3
	Conv2DTranspose	filter number	–	1
	MaxPooling2D	filter size	2×2	–
Training Parameters	Epoch		100	
	Optimizer		Adam	
	Loss function		MSE, MAE	
	Decay rate		0.98	
	Decap steps		1000	
	Learning rate		0.0005	

implemented on a 6-core CPU computer with an NVIDIA GeForce RTX 3090 GPU.

D. Electromagnetic Security Evaluation

The goal of EMSIM+ is to accelerate the traditional EM simulation process and predict EM data for EM leakage evaluation of ICs. The detailed steps are as follows. Input samples are provided to the generator of the well-trained EMSIM+, depending on data volumes required for the security evaluation. These samples include cell current maps, power grid maps, and time sequence. After that, the generator translates input feature maps into EM maps. In this paper, we carry out correlation EM analysis (CEMA) by traversing all grid tiles on the chip surface to analyze the EM leakage at each location of the chip, which assists in the security evaluation of ICs.

IV. EMSIM+ VS THE LATEST METHOD

To assess the credibility and effectiveness of EMSIM+ as a tool for evaluating EM side-channel security, we meticulously choose 4 exemplary cryptographic circuits, encompassing a range of cryptographic algorithms. Our experiments include conventional cryptography algorithms, post-quantum encryption algorithm, processor with extended instructions, and cryptography algorithm integrated with a protection scheme. In the first part, we perform a comprehensive analysis by comparing the simulation and evaluation results of EMSIM+ with those obtained using the latest EMSim tools, both in terms of accuracy and efficiency. Notably, for this evaluation, we employ the results obtained from EMSim as the ground truth values, which serve as the reference data for training the EMSIM+ model.

A. Experimental Setup

All 3 designs selected for this part are physically implemented utilizing SMIC 180 nm CMOS technology and run at a 25 MHz clock frequency and 1.8 V supply voltage. The feature extraction and training process of the EMSIM+ model have been thoroughly described Section III-A. The specific details of the 3 designs are presented below.

1) Kyber: This circuit occupies 1160 μm×1160 μm and implements the decryption function of the Crystals-Kyber algorithm, whose input private key and cipher text are both 24-bit. Kyber leverages shift registers to execute the Encode and Decode functions, and two sets of butterfly units to implement the Compress, Decompress, NTT, inverse NTT, and PWM functions.

2) AES_extension: This circuit occupies 900 μm×900 μm and implements an Instruction Set Architecture (ISA) extension for AES algorithm acceleration based on a 32-bit in-order AES_extension processor architecture.

3) AES_mask: This circuit occupies 1140 μm×840 μm, whose implementation draws inspiration from the renowned classical masking scheme proposed by Oswald et al. [15]. It uses a combination of additive and multiplicative masks to achieve a first-order SCA protection on the AES algorithm.

B. Accuracy Evaluation Metrics

To evaluate the accuracy of the proposed EMSIM+ in EM prediction and leakage evaluation, we use Normalized Cross-Correlation (NCC), Structural Similarity Index (SSIM) and evaluation error as the metrics. Each metric is defined as follows:

1) NCC reflects the accuracy of predicted EM data in temporal domains. It is computed according to Equation 4, where both the predicted EM data x, and the real EM data y, are normalized to the range of $[-1, 1]$. These normalized values are then represented by $\|x\|$ and $\|y\|$, each consisting of T time points. The cross correlation coefficients between $\|x\|$ and $\|y\|$ for N input stimuli is calculated and averaged to obtain the NCC result.

$$ncc = \frac{1}{N}\sum_{i=1}^{N}\frac{\sum_{t=1}^{T}\left(\|x\|_t^i - \|\bar{x}\|^i\right)\left(\|y\|_t^i - \|y\|^i\right)}{\sqrt{\sum_{t=1}^{T}\left(\|x\|_t - \|x\|^i\right)^2}\sqrt{\sum_{t=1}^{T}\left(\|y\|_t^i - \|y\|^i\right)^2}} \tag{4}$$

2) SSIM plays a role in comparing the similarity between the EM data x predicted by EMSIM+ and the real EM data y in three dimensions: luminosity l, contrast c and structural difference s. The calculation of these parameters is achieved following the formulation in Equation 5.

$$\begin{aligned} l(x,y) &= \frac{2\mu_x\mu_y + C_1}{\mu_x^2 + \mu_y^2 + C_1} \\ c(x,y) &= \frac{2\sigma_x\sigma_y + C_2}{\sigma_x^2 + \sigma_y^2 + C_2} \\ s(x,y) &= \frac{\sigma_{xy} + C_3}{\sigma_x\sigma_y + C_3} \end{aligned} \tag{5}$$

where (μx, μy), (σx, σx) and σxy are the average, standard deviation and covariance of x and y. C1, C2 and C3 are constants to avoid zero denominators. Under the conditions C3 = C2/2, the SSIM value is obtained by calculating the product of $l(x,y)$, $c(x,y)$ and $s(x,y)$ (see Equation 6).

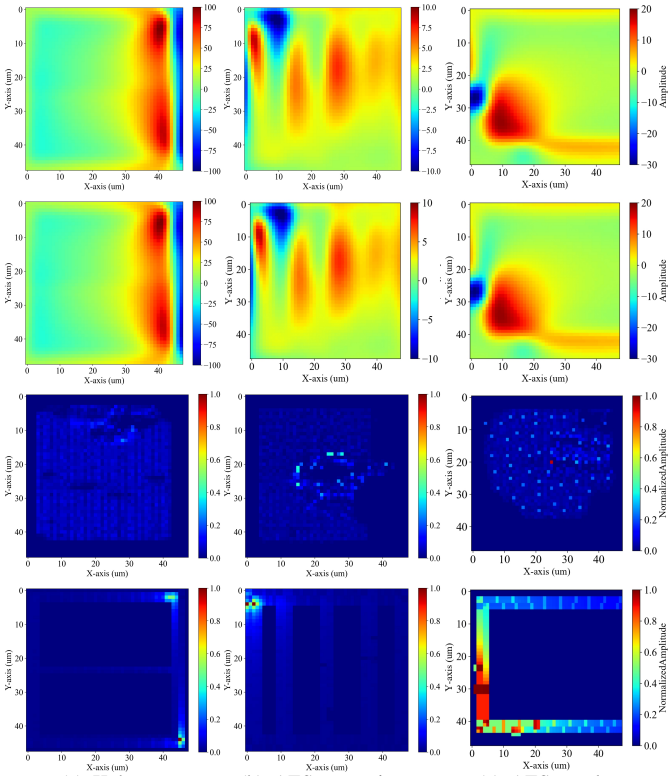
$$ssim = \frac{\left(2\mu_X\mu_Y + C_1\right)\left(2\sigma_{XY} + C_2\right)}{\left(\mu_X^2 + \mu_Y^2 + C_1\right)\left(\sigma_X^2 + \sigma_Y^2 + C_1\right)} \tag{6}$$

3) Evaluation error is applied to evaluate the results of the leakage evaluation. By exploiting evaluation error, we

can determine the correlation errors at information leakage hotspots.

C. EM Security Evaluation Results

1) EM emanations: Figure 6 presents a graphical representation of EM prediction results for the 3 designs at a specific time point. The first and second rows display the EM maps obtained through EMSim and the EM maps predicted by EMSIM+, respectively. In addition, the third and fourth rows exhibit the cell current maps and power grid maps used in EM information prediction at the same time point. These maps comprehensively contain the pertinent characteristics of cell current and power grid, thus providing a comprehensive and informative overview.

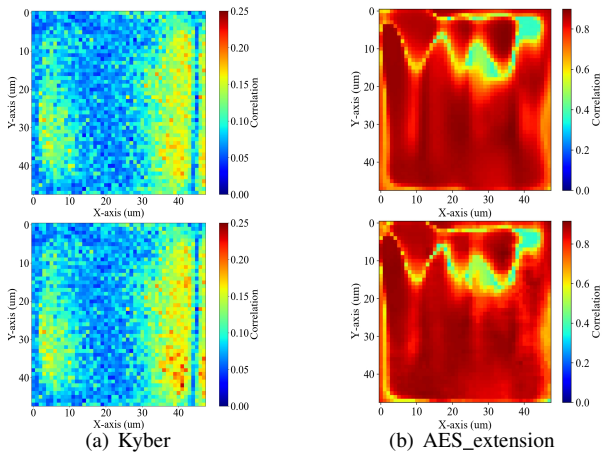


(a) Kyber (b) AES_extension (c) AES_mask

Fig. 6: EM map prediction results from EMSim and EMSIM+.

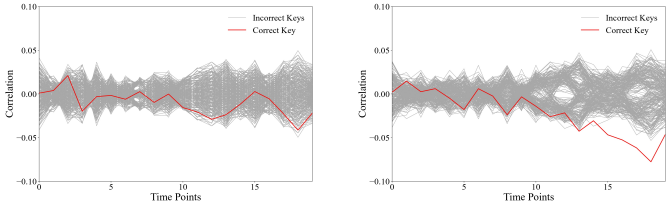
2) Security evaluation of Kyber and AES_extension: CEMA attacks are first executed on Kyber and AES_extension circuits, both are not equipped with side-channel protection. Despite using the Hamming distance (HD) value as the information leakage model, the vulnerabilities within these circuits manifest at distinct attack points. Specifically, Kyber targets the output of the point-by-point multiplication, while AES_extension focuses on registers for byte substitution operations during the first round of encryption. The results of EM data leakage analysis, generated by EMSim and EMSIM+ are presented as leakage maps in the first and second rows of Figure 7, respectively.

3) Security evaluation of AES_mask: Next, we undertake the prediction of 10 K EM traces to investigate the first-order



(a) Kyber (b) AES_extension

Fig. 7: EM leakage evaluation results of EMSim (top) and EMSIM+ (bottom) for Kyber and AES_extension.



(a) (b)

Fig. 8: EM leakage evaluation results of AES_mask with (a) HW model and (b) toggle-count model.

security of the AES_mask circuit against SCA. To accomplish this, we construct the Hamming weight (HW) matrix as an information leakage model by targeting the registers of the S-Box module. CEMA is carried out on AES_mask by systematically traversing all grid tiles positioned on the chip surface. Then, the correlation traces corresponding to key candidates are calculated at the targeted leakage hotspot. The result of the EM leakage evaluation is shown in Figure 8(a), affirming the robustness of the mask scheme in preserving the integrity of the correct key.

Further, we target the internal logic gates of the S-Box module, performing EM leakage analysis by constructing a toggle-count matrix as a leakage model. The result in Figure 8(b) demonstrates that 10 K traces are sufficient to reveal the correct key. Therefore, EMSIM+ not only assist in the diagnosis of potential security vulnerabilities in a circuit, but also serves as a tool for evaluating the efficacy of protection schemes.

4) Accuracy analysis: Table II shows the accuracy performance of EMSIM+ for the above designs. It can be seen that the NCC and SSIM metrics for EM prediction data exceed 99% with remarkable consistency. The performance evaluation of the leakage maps under the SSIM metric attains a threshold of over 95%, while maintaining an evaluation error of less than 0.02. The experimental results prove the robust learning ability of EMSIM+, which are on par with the well-established EMSim in terms of EM simulation accuracy.

TABLE II: Accuracy Performance of EMSIM+

Design	Kyber	AES_extension	AES_mask*
NCC	99.5%	99.9%	99.9%
SSIM of EM map	99.3%	99.8%	99.5%
SSIM of EM leakage map	97.0%	96.7%	95.0%
Evaluation error	0.01	0.01	0.02

* Accuracy analysis of AES_mask is calculated under the HW model.

D. Evaluation efficiency analysis

The accuracy of EMSIM+ has been demonstrated in above evaluation results. To further measure the efficiency of EMSIM+ comprehensively, we use Equation 7 and Equation 8 to calculate the time cost of both EMSim and EMSIM+ across different data volumes.

$$t\_EMSim = \frac{X}{1000}(F + L) \tag{7}$$

$$t\_EMSim+ = F + T + \frac{X}{1000}L \tag{8}$$

X denotes the total amount of data to be evaluated. For the circuits in the experiments, F, T and L represent the time spent on feature extraction, model training and leakage evaluation in minutes under 1 K data samples, respectively.

In Figure 9, we present the time cost analysis of EMSim and EMSIM+ across different data volumes (ranging from 1 K to 1 M traces) for various circuits. Notably, when dealing with 1 K traces, traditional EM simulation tool based on simulators EM leakage detection can adequately handle EM leakage evaluation. As the number of traces increases, the efficiency gap between the two methods becomes increasingly prominent. When the number of traces surpasses 10 K, EMSim's evaluation time extends to the scale of days, months, and even years, whereas EMSIM+ exhibits clear advantages in terms of efficiency. We introduce the ratio t_EMSim/t_EMSim+ to measure the efficiency improvement provided by EMSIM+ across different data volumes. Referring to the security level standard in ISO/IEC 17825-2016, security level III requires testing 10 K traces, EMSIM+ demonstrates an efficiency improvement of about $9.22 \sim 9.62$ times compared to EMSim. When upgraded to Security Levels IV, which requires 100 K traces, the evaluation efficiency is boosted by $73.48 \sim 86.05$ times. And for 1 M traces, the evaluation efficiency is remarkably improved by $242.60 \sim 419.35$ times.

V. EMSIM+ VS SILICON MEASUREMENT

To further demonstrate the capability of EMSIM+ in accurately simulating real chip EM emanation, we design and fabricate a chip named AES-128. In the second part, we use silicon measurements as ground truth to train the EMSIM+ model, enabling a comprehensive analysis of their results.

A. Experimental Setup

AES-128 implements the complete AES algorithm designed in compliance with the NIST standard with 128-bit input plaintext and key. The die area of the chip is 1.6 mm × 1.3 mm, and the supply voltage and clock frequency are set to 1.8V and 25 Mhz, respectively.

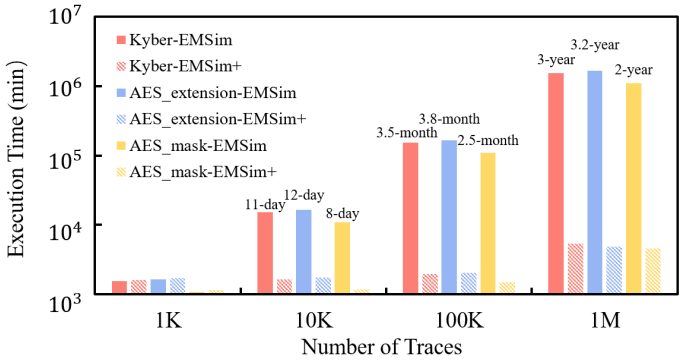


Fig. 9: Evaluation time cost of EMSim and EMSIM+ for different circuits under different number of traces.

To conduct the post-silicon leakage analysis of AES-128, we assemble an EM side-channel information acquisition platform. As illustrated in Figure 10, this setup comprises a three-axis positioning platform, ICR HH 250 -75 near-field probe, oscilloscope and a PC. The three-axis positioning platform precisely controls the probe to execute near-field scans of the IC surface. The probe has a resolution of 150 μm and an internal preamplifier to amplify the signal to +30 dB magnification. During the measurement, 1 K random plaintexts and a fixed key are loaded to AES-128 for encryption. The collected signal is sampled at 2.5 GSa/s and averaged over 32 measurements as the final EM data. These EM maps, together with cell current and power grid maps, serve as the dataset for training the EMSIM+ model from scratch, employing the parameters in Section III-C.

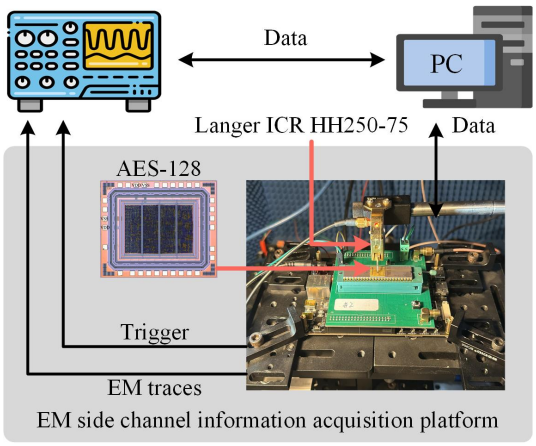
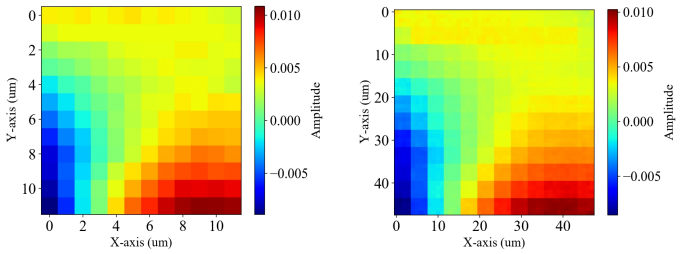


Fig. 10: The overview of the experimental setup.

B. EM Security Evaluation Results

1) EM emanations: As in Section IV-C, we chose a specific time point to construct the EM maps of the AES-128 chip surface. This time point corresponds to the clock cycle during which AES-128 executes a SubByte operation, targeting the first four bytes. The results of silicon measurements and

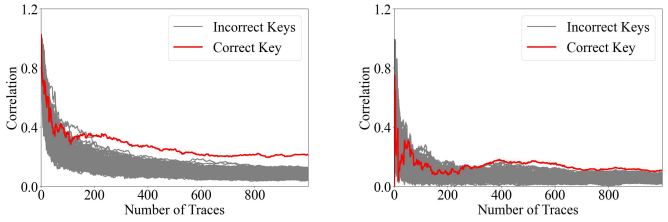


(a) Real EM map (b) Predicted EM map

Fig. 11: EM maps obtained by silicon measurements and EMSIM+.

EMSIM+ are represented in Figure 11(a) and 11(b), respectively. A remarkable consistency is observed in the distribution and amplitude of the EM information acquired through both silicon measurements and EMSIM+. The EM maps exhibit high fidelity, with NCC and SSIM metrics reaching 99.5% and 94.2%, respectively.

2) Security evaluation: We further evaluate the side-channel security of the chip by performing the CEMA attack described in Section III-D for each location on the chip surface. The attack results at the hotspots are translated into the MtD (measurement to disclosure) representation in Figure 12(a) and 12(b). For silicon measurements, $MtD \approx 173$ and for EMSIM+, $MtD \approx 265$. These experimental results validate the effectiveness of the trained EMSIM+ in precisely simulating the EM distribution of the real chip, leveraging layout-level cell current and power grid information.



(a) (b)

Fig. 12: MtD results of EM leakage evaluation of AES-128 by (a) silicon measurements and (b) EMSIM+.

VI. Discussion and Conclusion

In this paper, we present EMSIM+, a complete framework based on the GAN network for pre-silicon EM leakage detection of chips. EMSIM+ introduces ML into the EM security evaluation field for the first time, which significantly accelerates the process of layout-level EM simulation and leakage evaluation of large-scale ICs by learning transient mapping from cell current data and power grid data to EM data. The experimental results prove that EMSIM+ can accurately predict the EM information and evaluate the side-channel security. With 1 M traces, EMSIM+ has more than 242 times efficiency improvement compared to the latest method. In addition, comparison experiments between EMSIM+ and silicon measurements demonstrate that EMSIM+ can simulate real EM information by learning the difference between simulation and real measurements at post-silicon stage.

Acknowledgements

This work is supported in part by the National Key R&D Program of China (Grant No. 2021YFB3100903).

References

[1] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Annual International Cryptology Conference*. Springer, 1999, pp. 388–397.

[2] Y. Zhao, S. Pan, H. Ma, Y. Gao, X. Song, J. He, and Y. Jin, "Side channel security oriented evaluation and protection on hardware implementations of kyber," *IEEE Transactions on Circuits and Systems I: Regular Papers*, 2023.

[3] K. Monta, L. Lin, J. Wen, H. Shrivastav, C. Chow, H. Chen, J. Geada, S. Chowdhury, N. Pundir, N. Chang, and M. Nagata, "Silicon-correlated simulation methodology of em side-channel leakage analysis," *ACM Journal on Emerging Technologies in Computing Systems*, vol. 19, 10 2022.

[4] M. Ramdani, E. Sicard, A. Boyer, S. B. Dhia, J. J. Whalen, T. H. Hubing, M. Coenen, and O. Wada, "The electromagnetic compatibility of integrated circuits—past, present, and future," *IEEE Transactions on Electromagnetic Compatibility*, vol. 51, no. 1, pp. 78–100, 2009.

[5] Y. Gao, Q. Zhang, H. Ma, J. He, and Y. Zhao, "EO-Shield: A multi-function protection scheme against side channel and focused ion beam attacks," in *Proceedings of the 28th Asia and South Pacific Design Automation Conference*, 2023, pp. 670–675.

[6] H. Li, A. T. Markettos, and S. Moore, "Security evaluation against electromagnetic analysis at design time," in *High-Level Design Validation and Test Workshop, 2005. Tenth IEEE International*, 2005, pp. 211–218.

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

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

[9] H. Ma, M. Panoff, J. He, Y. Zhao, and Y. Jin, "EMSim: A fast layout level electromagnetic emanation simulation framework for high accuracy pre-silicon verification," *IEEE Transactions on Information Forensics and Security*, 2023.

[10] Q. Fang, L. Lin, Y. Z. Wong, H. Zhang, and M. Alioto, "Side-channel attack counteraction via machine learning-targeted power compensation for post-silicon hw security patching," in *2022 IEEE International Solid-State Circuits Conference (ISSCC)*, vol. 65, 2022, pp. 1–3.

[11] M. B. Alawieh, W. Li, Y. Lin, L. Singhal, M. A. Iyer, and D. Z. Pan, "High-definition routing congestion prediction for large-scale fpgas," in *2020 25th Asia and South Pacific Design Automation Conference (ASP-DAC)*. IEEE, 2020, pp. 26–31.

[12] Y.-C. Lu, J. Lee, A. Agnesina, K. Samadi, and S. K. Lim, "GAN-CTS: A generative adversarial framework for clock tree prediction and optimization," in *2019 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*. IEEE, 2019, pp. 1–8.

[13] V. A. Chhabria, V. Ahuja, A. Prabhu, N. Patil, P. Jain, and S. S. Sapatnekar, "Thermal and ir drop analysis using convolutional encoder-decoder networks," in *Proceedings of the 26th Asia and South Pacific Design Automation Conference*, 2021, pp. 690–696.

[14] I. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, and Y. Bengio, "Generative adversarial networks," *Communications of the ACM*, vol. 63, no. 11, pp. 139–144, 2020.

[15] E. Oswald, S. Mangard, N. Pramstaller, and V. Rijmen, "A side-channel analysis resistant description of the AES S-box," in *International workshop on fast software encryption*. Springer, 2005, pp. 413–423.