EMSIM+: Accelerating Electromagnetic Security Evaluation With Generative Adversarial Network and Transfer Learning

Ya Gao, Haocheng Ma, Qizhi Zhang, Xintong Song, Yier Jin, *Senior Member, IEEE*, Jiaji He, and Yiqiang Zhao

***Abstract*— Electromagnetic side-channel analysis (EM SCA) attack poses a serious threat to integrated circuits (ICs), necessitating timely vulnerability detection before deployment to enhance EM side-channel security. Various EM simulation methods have emerged for analyzing EM side-channel leakage, providing sufficiently accurate results. However, these simulator-based methods still face two principal challenges in the design process of high security chips. Firstly, the large volume of measurement data required for a single security evaluation results in substantial time overhead. Secondly, design iterations lead to repetitive security evaluations, thus increasing the evaluation cost. In this paper, we propose EMSIM+ which includes two efficient and accurate layout-level EM side-channel leakage evaluation frameworks named EMSIM+GAN and EMSIM+GAN+TL to mitigate the above challenges, respectively. EMSIM+GAN integrates a Generative Adversarial Network (GAN) model that utilizes the chip's cell current and power grid information to predict EM emanations quickly. EMSIM+GAN+TL further incorporates transfer learning (TL) within the framework, leveraging the experience of existing designs to reduce the training datasets for new designs and achieve the target accuracy. We compare the simulation results of EMSIM+ with the state-of-the-art EM simulation tool, EMSIM as well as silicon measurements. Experimental results not only prove the high efficiency and high simulation accuracy of EMSIM+, but also verify its generalization ability across different designs and technology nodes.**

***Index Terms*— CAD for security, side-channel analysis, generative adversarial network, transfer learning.**

I. INTRODUCTION

OVER the past two decades, side-channel analysis (SCA) attacks have posed a serious threat to the information security of integrated circuits (ICs) [1]. Through the collection and analysis of information inadvertently emitted by ICs, such as electromagnetic (EM) emanations, power consumption, and timing deviations, SCA attacks can compromise the confidentiality of targeted ICs, leading to the leakage of cryptographic chip keys or neural network model parameters [2]. Given these risks, it is necessary to assess the side-channel security of ICs before deployment. Typically, security evaluations happen after the chip fabrication. Failing to meet security standards incurs expensive revision costs and delays time-to-market. Therefore, it is highly desirable to implement side-channel evaluations at the early design stage, allowing designers to identify and modify security vulnerabilities with more flexibility [3].

Among various side-channel information, EM emanations originate from the current inside the ICs' components and contain a wealth of information in the spatial, temporal, and frequency domains. Nowadays, EM SCA attacks have emerged as one of the most destructive security threats [4], [5]. In response, designers combine EM simulations with SCA techniques to evaluate side-channel vulnerabilities of ICs at the layout phase. To achieve this goal, many methods have been proposed to speed up EM simulations while maintaining the high accuracy of simulated results. Li et al. pioneered the EM simulation flow to predict global information leakage from different processors during the layout phase. This flow includes current flow simulation, layout parasitic extraction, and EM emanation calculation [6]. Lomné et al. advanced the EM simulation by modeling the transient currents of power and ground networks, contributing to the prediction of spatial information leakage [7]. As the scale of ICs increases, the complexity of device models and parasitic networks grows rapidly, leading to challenges such as time explosion in EM simulations. To address these challenges, there have been several tools and techniques proposed in the literature. Kumar et al. mixed the gate-level and transistor-level current simulations and only retained the current data from the top-level power-delivery network. With the help of Synopsys FineSim's parallel mechanism, they accelerated the computation of EM emanations [8]. Ma et al. developed the tool, i.e., EMSIM, which reduces the computational complexities through parasitic network reduction and device model approximation [9]. Compared to traditional EM simulation at the layout level, EMSIM achieves a $\sim 32\times$ increase in efficiency while maintaining high accuracy.

When designing a high-security chip, two main challenges persist in the practical application of existing EM simulations for security evaluations. **First, a single security evaluation**

Received 26 March 2024; revised 29 August 2024; accepted 13 October 2024. Date of publication 18 October 2024; date of current version 29 October 2024. This work was supported in part by the National Key Research and Development Program of China under Grant 2023YFB4402800 and Grant 2023YFB4403000 and in part by the Natural Science Foundation of Tianjin under Grant 22JCQNJC00970. The associate editor coordinating the review of this article and approving it for publication was Dr. Mohammad Ashiqur Rahman. *(Corresponding authors: Jiaji He; Yiqiang Zhao.)*

Ya Gao, Haocheng Ma, Qizhi Zhang, Xintong Song, Jiaji He, and Yiqiang Zhao are with the School of Microelectronics, Tianjin University, Tianjin 300072, China (e-mail: gaoyaya@tju.edu.cn; hc_ma@tju.edu.cn; qizhi_zhang@tju.edu.cn; xintong_song@tju.edu.cn; dochejj@tju.edu.cn; yq_zhao@tju.edu.cn).

Yier Jin is with the School of Cyber Science and Technology, University of Science and Technology of China, Hefei 230026, China (e-mail: yier.jin@ustc.edu.cn).

Digital Object Identifier 10.1109/TIFS.2024.3483551

often requires to collect more than hundreds of thousands or even millions of traces, bringing a significant time overhead on simulator-based methods. Taking EMSIM as an example, the simulator solves large-scale systems of nonlinear equations to calculate EM data. The time cost of this computation grows exponentially as the sample size increases. When the EM data required for security evaluation reaches around 100K, the simulation time for EMSIM will extend to several months. **Second, version iterations of a chip during the design phase require designers to continually re-perform security evaluations to identify potential security risks, which further imposes a heavy time burden.**

In recent years, machine learning (ML) has advanced into fields such as Electronic Design Automation (EDA) and chip manufacturability by providing fast and high-quality solutions to time- or resource-intensive mathematical analysis and computation processes. In this paper, we develop a framework named EMSIM+,[1] including two ML-based frameworks, EMSIM+GAN and EMSIM+GAN+TL, to address the challenges aforementioned in EM security evaluation, respectively. Figure 1 illustrates the difference between the general flow and EMSIM+ flow. In the general flow, EM emanations used for evaluation are obtained through the general method. Here we define general method as traditional EM simulation tools like EMSIM or silicon measurements. EMSIM+GAN flow contains a Generative Adversarial Network (GAN) model, which is capable of generating new data with additional information from the original data and is widely used for data prediction tasks. EMSIM+GAN first gathers a small set of sample pairs from the general method. These sample pairs range from cell currents and power grids to EM traces and serve as ground truth data to train the GAN model. By utilizing the predictive power of GANs, EMSIM+GAN significantly accelerates the generation of EM evaluation data, thus addressing the extensive time requirements identified in our first challenge. EMSIM+GAN+TL incorporates transfer learning (TL) into the EMSIM+GAN framework. TL minimizes the necessity for large training datasets by applying previously acquired knowledge. It is easy to quickly update models for different design versions without having to be an AI expert, thus effectively mitigating the time constraints associated with security evaluations during design iterations, as outlined in our second challenge.

The main contributions of this paper are highlighted as follows.

- A fast layout-level EM side-channel security evaluation framework, named EMSIM+, is developed and evaluated. EMSIM+ utilizes ML in EM security evaluation for the first time. It contains two frameworks, EMSIM+GAN and EMSIM+GAN+TL, facilitating more efficient and security-focused evaluations of designs.
- The input feature maps of EMSIM+ are extracted from the layout-level design, where the maps contain information about the cell current and power grid that cause the source of EM emanations. Using continuous time as one of the conditions, EMSIM+GAN harnesses GANs' image-to-image translation capability to learn EM variations over time.
- EMSIM+GAN+TL further incorporates a TL approach to significantly reduce the training duration and data volume by leveraging insights derived from other circuits. This strategy effectively bypasses the limitations associated with specific designs or technology nodes, substantially enhancing its versatility and adaptability across diverse design spaces.
- We apply EMSIM+ to a representative set of cryptographic circuits and compare the results with the state-of-the-art EM simulation tool, EMSIM and silicon measurements. Experimental results demonstrate that EMSIM+ maintains comparable accuracy to EMSIM. For EM leakage evaluation under 1M sample data, EMSIM+ improves the efficiency over $\sim$ 242$\times$ compared to EMSIM.

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

II. BACKGROUND

A. ML-Based Electronic Design Automation (EDA)

Driven by Moore's Law, the complexity and scale of ICs are increasing rapidly, bringing significant challenges in terms of circuit performance and security. Traditional EDA tools typically rely on rule-based and deterministic algorithms to complete IC designs. Due to the lack of knowledge accumulation, these tools have to execute each task from scratch, thus making it harder to meet the demands of escalating ICs' complexity and the need for faster design cycles. In contrast, ML algorithms are adept at extracting valuable insights from large datasets and reusing them under relevant tasks. Benefiting from data-driven models, ML offers a fast, high-quality approach to these challenges.

Currently, the application of ML in optimizing EDA tools extends to almost all stages of ICs' design, yielding predictions that rival the accuracy of traditional methods. Alawieh et al. translated placement schemes and the connectivity information as input images to speed up forecasting routing congestion map for large-scale FPGA via a Conditional GAN (CGAN) [10]. Lu et al. proposed 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 [11]. Chhabria et al. utilized an encoder-decoder-based CGAN to perform thermal analysis and IR drop prediction based on potential characteristics of power distribution and density [12]. The above ML-based analysis methods replace the multi-step, high-complexity solution processes and demonstrate an impressive ability to improve the efficiency of each sub-task, even surpassing traditional methods. With the help of ML,

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

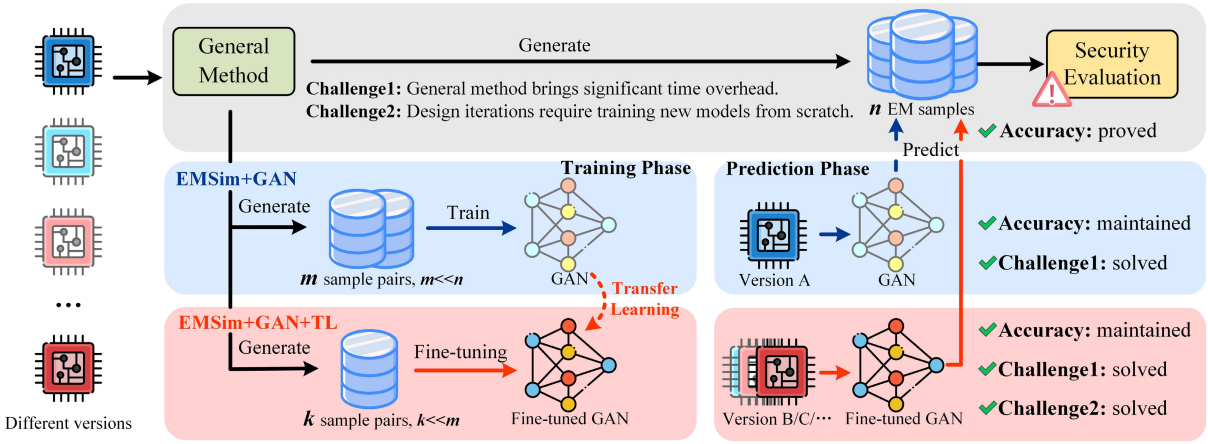


Fig. 1. General flow vs. EMSIM+ flow.

designers can dramatically reduce the time and effort required to design and verify IC 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 [13], 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 uses 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 transposing convolution layers in the decoder. D is 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 Equation (1):

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

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

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 grid information through GAN. Therefore, the CGAN model is especially suitable for this task. It can accept input feature maps with additional samples, allowing for generating more precise samples.

C. Transfer Learning (TL)

Traditional ML algorithms typically work within the same feature space or distribution. When the distribution changes,

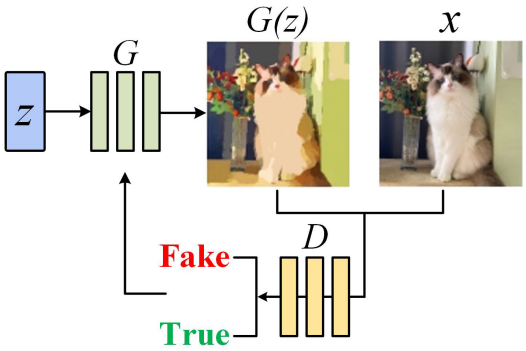


Fig. 2. The structure of a generative adversarial network.

the performance of the well-trained model often decreases. In that case, the model needs to be rebuilt with the new data from the new domain. In contrast, TL can apply knowledge from one or multiple source domains to a target domain. It doesn't need to train the new model from scratch, thus offering a more adaptable and robust approach [14]. By utilizing knowledge acquired from diverse but related source tasks or domains, TL will fine-tune the model to fit the target task [15], [16]. The concept of TL involves two fundamental domains and two tasks: the source domain (D_s) and the target domain (D_t), as well as the source task (T_s) and the target task (T_t). The basic assumption of TL is that when $D_s \neq D_t$ or $T_s \neq T_t$, the 'knowledge' derived from D_s—encompassing data features, model parameters, etc.—can assist the learning process of T_t within D_t. Typical TL schemes such as Fine-tuning usually freeze the initial layers of the model trained for D_s and adjust the subsequent layers with data from D_t. The initial layers capture similar features between D_s and D_t, while the subsequent layers serve as classifiers or regressors requiring fine-tuning.

Due to the complexity of IC designs and manufacturing processes, it is highly costly to obtain sufficient training data with acceptable accuracy for ML-based EDA tools. This challenge becomes more serious due to the intensive exploration of the design space and the continuous evolution of tech-

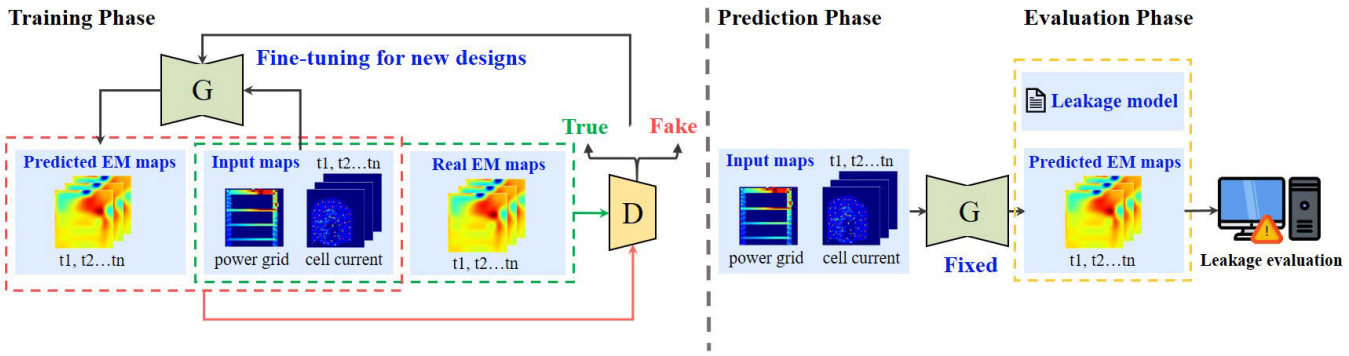


Fig. 3. The proposed EMSIM+ framework.

nology process nodes. Therefore, it's important to minimize the need for expensive datasets and to accelerate the model construction. Several studies have explored the effectiveness of using TL for knowledge transfer across different process nodes. For instance, Lin et al. proposed a TL-based resist modeling framework for contact layers [17]. By transferring common knowledge between old and new process nodes, this framework reduced the quantity of data required from the target lithography configuration. Similarly, Gai et al. constructed a layout hotspot detection model with TL to evaluate the reliability of ICs, which significantly reduced the consumption cost required for wafer verification at different process nodes [18].

In the context of EMSIM+, circuits with different functions or technology process node implementations can be considered as separate T_ts in different D_ts. Our approach suggests to choose Fine-tuning. By freezing the discriminator using the best pre-trained model from T_s and fine-tuning the generator with data from D_t, the optimal performance of EMSIM+ is achieved. In this way, researchers can avoid training models from scratch repeatedly when facing frequent design changes or process iterations. We believe that TL mitigates EMSIM+'s dependence on specific designs or process nodes, further improving the efficiency of EM security evaluations and alleviating the time explosion challenge in traditional EM simulation methods.

III. Proposed EMSIM+ Framework

The overview of the proposed EMSIM+ is shown in Figure 3, including the training phase, prediction phase, and evaluation phase. For a design under evaluation, EMSIM+GAN designs and trains a GAN model for EM prediction during the training phase. Specifically, the generator G accepts three types of input features extracted from the circuit, which are cell current maps, power grid maps, and time sequences. 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 improve the quality of predicted EM maps. During the prediction phase, G is fixed and serves as an inference model for EM prediction. By providing the inference model with cell current maps and power grid maps, EM maps required for evaluation can be predicted. Eventually, the evaluation phase gives feedback on whether the circuit has the risk of EM side-channel leakage. For the modified design, i.e., a new design, we reevaluate its security using EMSIM+GAN+TL. During the training phase, D is frozen and G is fine-tuned by a limited dataset to construct a new model, and the prediction and evaluation phases are subsequently repeated. Here we focus on the details of the feature extraction, architecture design, model training, and EM security evaluation process in EMSIM+.

A. Feature Extraction

Based on the theoretical model of EM emanations from ICs in [9], the transient current data of logic cells and the topmost power grid are the sources of EM emanations. Therefore, we first extract the cell current and power grid information from the database of the chip's physical layout. We convert them into feature maps and then combine them as input feature maps for G. Next, EM data is extracted by general 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 an $l \times l$ 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, $i = 1, 2, \ldots\ldots n$, 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

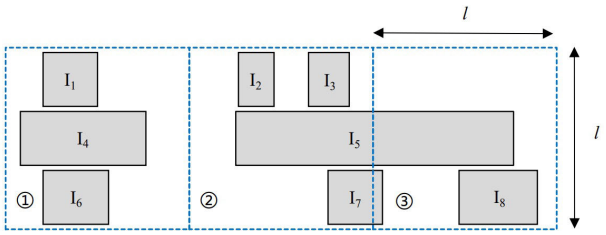


Fig. 4. Space decomposition of cell currents.

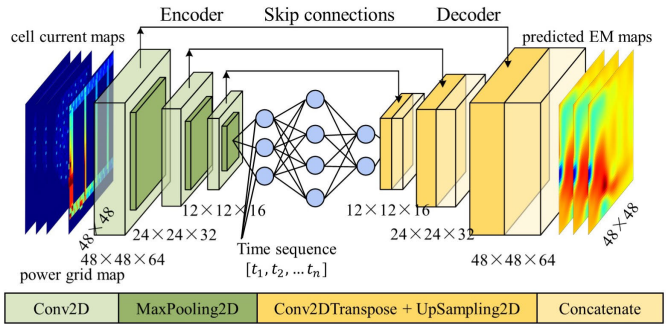


Fig. 5. The generator network of EMSIM+.

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):

$$d = |x_1 - x_2| + |y_1 - y_2| \tag{2}$$

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).

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

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.

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 as well as a power grid map before converting them 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 downsampling 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 the realness of EM map inputs. 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

Figure 6 illustrates the training scheme for our proposed EMSIM+. For T_s, we choose EMSIM+GAN flow to train a GAN model from scratch using the dataset from D_s. The training parameters, such as pixel dimensions of input feature maps, simulation time points, filter size, and even the dataset division, can be adjusted to accommodate various situations, enhancing the model's scalability. For T_t, we switch to EMSIM+GAN+TL flow and use the fine-tuning method introduced in Section II-C for TL. All the best pre-trained parameters from the GAN model of T_s are initially shared with the target GAN model. During the training phase, we freeze the discriminator of the target GAN model by fixing its parameters. Subsequently, we fine-tune the generator's parameters using a small subset of training data from D_t to achieve the desired accuracy.

As a proof of concept, we consider input and output feature maps with dimensions of 48×48 pixels, and hyperparameters used for model training are tabulated in Table I. Note that the model is trained based on pixel resolution, requiring retraining for different resolution sizes. The model remains suitable for various chip sizes as long as the resolution size remains consistent. The analysis period is assumed to be 20 ns, represented as a time sequence of 20. Before the

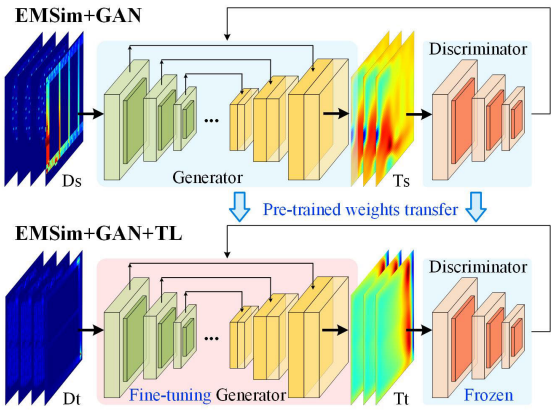


Fig. 6. Training process of EMSIM+.

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	

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 developed and evaluated in TensorFlow2.4. Both training and testing are implemented on a 6-core CPU computer with an NVIDIA GeForce RTX 3090 GPU.

D. Electromagnetic Security Evaluation

The final step of EMSIM+ is EM security evaluation. In the context of side-channel security evaluation, common methods are mainly divided into two categories: attacking-style evaluations such as Correlation Electromagnetic Analysis (CEMA), and leakage detection-style evaluation, represented by Test Vector Leakage Assessment (TVLA) [19], [20]. Given that TVLA involves statistical analysis of random variables, it is susceptible to get false positive or negative results. Conversely, attacking-style evaluation is more suitable for comprehensive analysis of cryptographic algorithms, which facilitates vulnerability identification and the development of protection schemes. Consequently, EMSIM+ uses CEMA for security evaluation, utilizing Pearson's correlation coefficient and Minimum number of Traces to Disclosure (MtD) as security metrics.

CEMA is a widely used SCA method that utilizes the Pearson correlation between the real EM traces (matrix T) and the hypothesized leakage model (matrix H) to screen the true keys. Here the real EM traces are simulated through EMSIM+, the leakage model is constructed from the guessed key and known plaintexts using the Hamming distance (HD) or Hamming weight (HW) model. The correlation matrix R is calculated as depicted in Equation (4).

$$r_{i,j} = \frac{\sum_{d=1}^{D}(h_{d,i} - \bar{h}_i) \cdot (t_{d,j} - \bar{t}_j)}{\sqrt{\sum_{d=1}^{D}(h_{d,i} - \bar{h}_i)^2 \cdot (t_{d,j} - \bar{t}_j)^2}} \tag{4}$$

where t and h come from matrix T and H, respectively, and d is usually a partial plaintext. Theoretically, the true key has the highest correlation value r.

In the security evaluation, depending on the amount of data required, we provide cell current maps, power grid maps, and the time sequence to the generator of the well-trained EMSIM+. The generator then translates input feature maps into EM maps. We carry out 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+GAN VS THE LATEST METHOD

To validate that EMSIM+ enables accurate and fast EM side-channel security evaluation, we choose 3 exemplary cryptographic circuits for experiments, including various cryptographic algorithms (conventional cryptographic algorithms, post-quantum encryption algorithms, and a processor with extended instructions). Here we perform a single security evaluation for different circuits, so we choose the EMSIM+GAN flow. We comprehensively compare the evaluation results of EMSIM+GAN with the state-of-the-art EMSIM tool in terms of both accuracy and efficiency. In [9], the computational results of EMSIM have been fully compared to post-silicon measurements, demonstrating its high-precision EM simulation capabilities. Therefore, in this section, we use the results obtained by EMSIM as ground truth values to train the GAN model of EMSIM+GAN.

A. Experimental Setup

Table II lists the key information used for feature extraction in 3 selected experimental designs. Specifically, it includes the area, the number of logical cells used to extract cell current maps, and the number of top metal wires used to extract the power grid maps. All designs are physically implemented utilizing SMIC 180 nm CMOS technology and run at a 25 MHz clock frequency and 1.8 V supply voltage. The specific details of the 3 designs are presented below.

1) AES: This circuit implements the complete AES algorithm designed in compliance with the NIST standard with 128-bit input plaintext and key.

TABLE II
DESIGNS USED IN EXPERIMENT I

Design \ Feature	Area (μm^2)	Logical cells	Top metal wires
AES	1140 × 840	14559	1424
Kyber	1160 × 1160	14598	587
AES_extension	900 × 900	11660	870

2) Kyber: This circuit 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.

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

For the above designs, the process of feature extraction and model training is described in Section III-A. We treat each design as a T_s and extract 1K sample pairs to train the GAN model from scratch. In the evaluation phase, an additional 1K pairs of cell current and power grid maps are produced, and the trained GAN model is used to predict EM maps and perform EM leakage evaluation.

B. Accuracy Evaluation Metrics

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

1) Generator Loss: reflects the performance of the generator and the quality of the generated samples. It consists of two loss functions in the GAN model, MSE and MAE, which are calculated as in Equation (5). The contribution of MSE and MAE to Generator loss is balanced by assigning weights 1 and 100. A reduction in the generator loss means the generated samples are more realistic, thus meeting the task requirements. Conversely, an increase may suggest a growing difference between the generated and real samples, requiring further adjustments to the generator parameters.

$$generator\_loss = mse\_loss + 100 \times mae\_loss \tag{5}$$

2) NCC: reflects the accuracy of the prediction data in the time domain. It is computed according to Equation (6), 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 are calculated and averaged to obtain the NCC result.

$$ncc = \frac{1}{N}\sum_{i=1}^{N}\frac{\sum_{t=1}^{T}\left(\|x\|_t^i - \|\bar{x}\|^i\right)\left(\|y\|_t^i - \|y\|^i\right)}{\sqrt{\sum_{t=1}^{T}\left(\|x\|_t - \|x\|^i\right)^2}\sqrt{\sum_{t=1}^{T}\left(\|y\|_t^i - \|y\|^i\right)^2}} \tag{6}$$

3) SSIM: measures the accuracy of the prediction data in spatial domain in terms of three dimensions: luminosity l, contrast c and structural difference s. The calculation of these parameters is achieved following the formulation in Equation (7).

$$\begin{aligned} l(x,y) &= \frac{2\mu_x\mu_y + C_1}{\mu_x^2 + \mu_y^2 + C_1} \\ c(x,y) &= \frac{2\sigma_x\sigma_y + C_2}{\sigma_x^2 + \sigma_y^2 + C_2} \\ s(x,y) &= \frac{\sigma_{xy} + C_3}{\sigma_x\sigma_y + C_3} \end{aligned} \tag{7}$$

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 (8)). A relatively large NCC and SSIM value indicates a high similarity between EM maps, which will lead to a satisfactory model prediction.

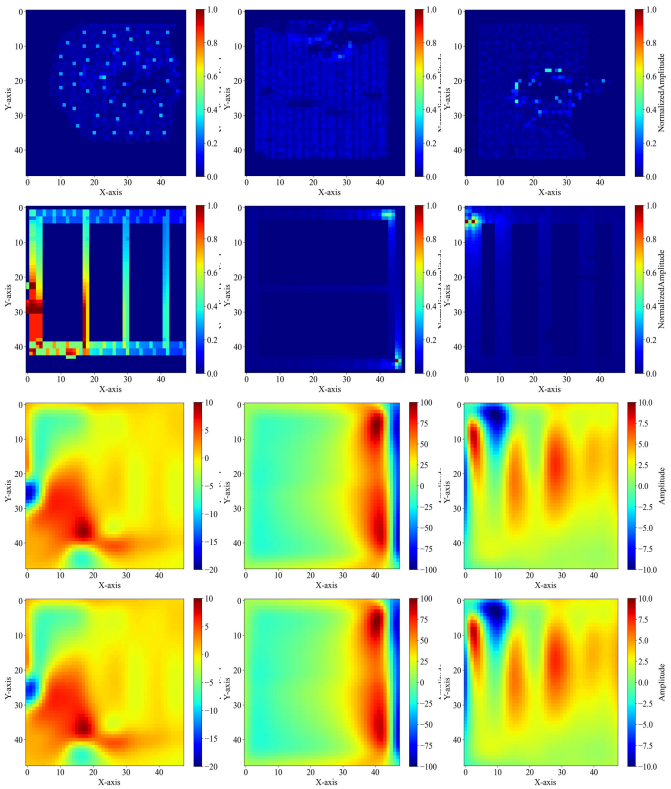
$$ssim = \frac{(2\mu_X\mu_Y + C_1)(2\sigma_{XY} + C_2)}{(\mu_X^2 + \mu_Y^2 + C_1)(\sigma_X^2 + \sigma_Y^2 + C_1)} \tag{8}$$

4) Evaluation Error: is applied to evaluate the results of the leakage evaluation. We can determine the correlation errors at information leakage hotspots through evaluation errors. Smaller evaluation errors mean higher accuracy for EMSIM+.

C. EM Security Evaluation Results

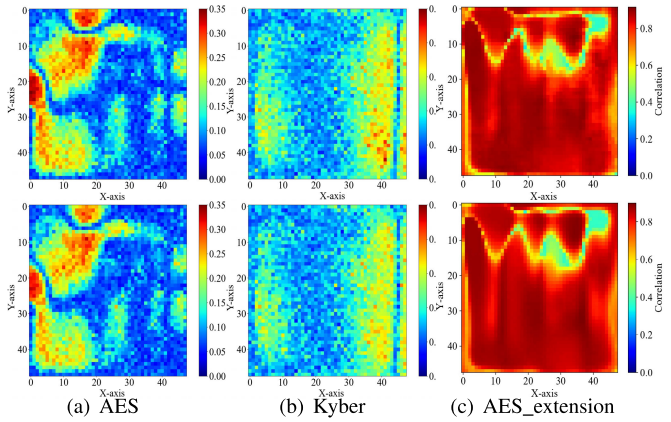
1) EM Emanations: Figure 7 visualizes EM prediction results for the 3 designs at a specific time point in the form of heat maps. Red color indicates higher values while blue corresponds to lower values. The first and second rows depict cell current maps and power grid maps extracted from the layout level at the same time point, respectively. In EMSIM, these maps are utilized to compute EM maps (third row of Figure 7). While in EMSIM+GAN, these maps serve as input feature maps for the generator to predict EM maps (fourth row of Figure 7). The comparison reveals that EM maps obtained from EMSIM and EMSIM+GAN have similar amplitude ranges at each position of the layout.

2) Security Evaluation: We adopt the CEMA introduced in Section III-D to perform EM security evaluation, thus determining whether the generated EM traces can preserve the key information leakage found in the original EM traces. This will allow us to evaluate the accuracy of EMSIM+ and see if it has the potential to replace traditional EM simulation tools such as EMSIM. Despite using the Hamming distance (HD) value as the information leakage model, the vulnerabilities in these circuits are located at different attack points. Specifically, AES and AES_extension focus on registers for byte substitution operations during the first round of encryption, while Kyber targets the output of the point-by-point multiplication. The leakage analysis results obtained by EMSIM and EMSIM+GAN are presented as leakage maps in the first and second rows of Figure 8, respectively. These results exhibit high similarity in terms of correlation hotspot distributions and values.



(a) AES (b) Kyber (c) AES_extension

Fig. 7. EM map prediction results from EMSIM and EMSIM+GAN.



(a) AES (b) Kyber (c) AES_extension

Fig. 8. EM leakage evaluation results of EMSIM (top) and EMSIM+GAN (bottom).

3) Accuracy Analysis: Table III shows the accuracy performance of EMSIM+GAN for the above designs. 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. Experimental results show that EMSIM+GAN can be used as a highly accurate leakage evaluation tool to identify security vulnerabilities.

D. Evaluation Efficiency Analysis

To further measure the efficiency of EMSIM+ comprehensively, we use Equation (9) and (10) to calculate the time cost of both EMSIM and EMSIM+GAN across different data volumes.

$$t_{EMSim} = \frac{X}{1000}(F + L) \tag{9}$$

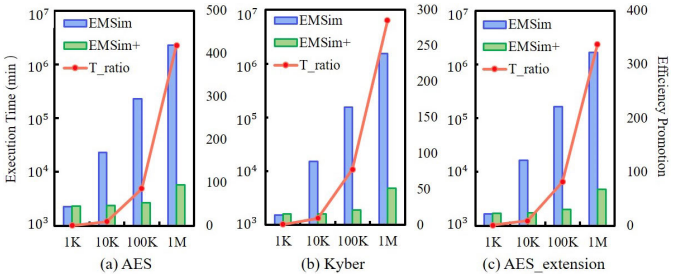
$$t_{EMSim+GAN} = F + T + \frac{X}{1000}L \tag{10}$$

X denotes the total samples for evaluation. F, T and L represent the time spent on feature extraction, model training and leakage evaluation in minutes under 1 K data samples, respectively.

Figure 9 shows the execution times in minutes of EMSIM and EMSIM+GAN for different circuits and data volumes (ranging from 1 K to 1 M traces) using bar charts. Additionally, the efficiency promotion value of EMSIM+GAN is quantified using the time ratio $T\_ratio = t_{EMSim}/t_{EMSim+GAN}$, which is depicted in Figure 9 via a broken line. Obviously, when dealing with 1 K traces, traditional EM simulation tool based on simulators can adequately handle EM security evaluation. As the number of traces increases, the efficiency gap between the two methods becomes increasingly prominent. Beyond 10 K traces, EMSIM's evaluation time extends to the scale of days, months, and even years, whereas EMSIM+GAN exhibits clear advantages in terms of efficiency. Referring to the security level standard in ISO/IEC 17825-2016, Security Level III requires testing 10 K traces, EMSIM+GAN demonstrates an efficiency improvement of about 9.22 $\sim$ 9.62 times compared to EMSIM. When upgraded to Security Level IV, which requires 100 K traces, the evaluation efficiency is boosted by 73.48 $\sim$ 86.05 times. Moreover, for 1 M traces, the evaluation efficiency is remarkably improved by 242.60 $\sim$ 419.35 times.

TABLE III
ACCURACY PERFORMANCE OF EMSIM+GAN

Metric \ Design	AES	Kyber	AES_extension
Generator loss	5.7996e-04	2.7735e-04	9.0921e-04
NCC	99.2%	99.5%	99.9%
SSIM of EM map	99.6%	99.3%	99.8%
SSIM of EM leakage map	95.1%	97.0%	96.7%
Evaluation error	0.02	0.01	0.01



(a) AES (b) Kyber (c) AES_extension

Fig. 9. Efficiency comparison between EMSIM and EMSIM+GAN across different circuits and number of traces.

V. EMSIM+GAN VS SILICON MEASUREMENT

To further demonstrate the capability of EMSIM+ in accurately simulating real chip's EM emanations, we design and fabricate a chip named AES-128 that implements the AES

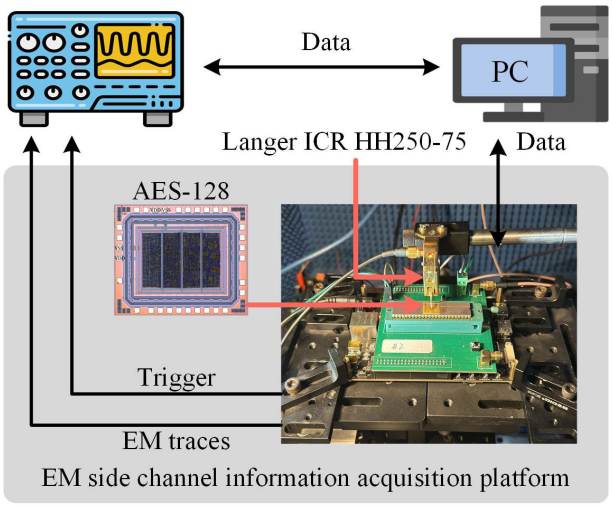
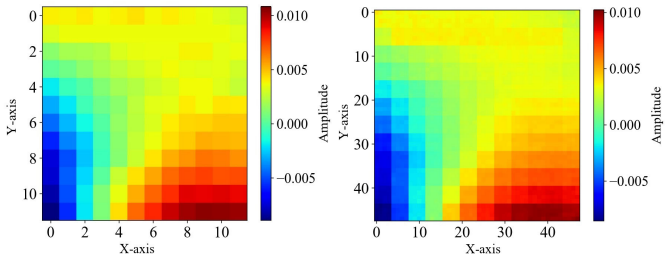
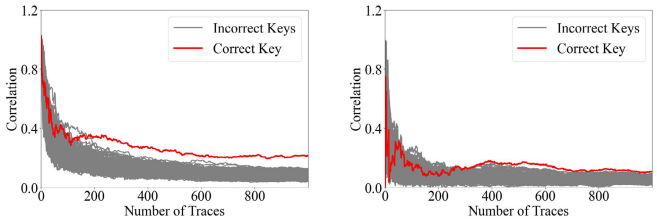


Fig. 10. The overview of the experimental setup.



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

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



(a) (b)

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

circuit in Section IV. Silicon measurements are used as ground truth to train the GAN model of EMSIM+GAN from scratch.

A. Experimental Setup

The die area of the AES-128 chip [9] is 1.6 mm × 1.3 mm, and the supply voltage and clock frequency are set to 1.8V and 25 Mhz, respectively. To collect the EM traces during the operation of AES-128, we assemble an EM side-channel information acquisition platform as shown in Figure 10. This setup comprises a three-axis positioning platform, an ICR HH 250 -75 near-field probe, an oscilloscope, and a PC. The three-axis positioning platform precisely controls the probe to execute near-field scans of the IC surface with a step of 80 μm. 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 extracted by EMSIM, serve as the dataset for training the GAN model of EMSIM+GAN from scratch, employing the parameters in section III-C.

B. EM Security Evaluation Results

1) EM Emanations: We choose a specific time point to construct 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 EMSIM+GAN 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+GAN. 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 CEMA for each location on the chip surface. The attack results at the hotspots are translated into the MtD representation in Figure 12(a) and 12(b). For silicon measurements, $MtD \approx 173$ and for EMSIM+GAN, $MtD \approx 265$. Due to the test noise, EM interference, and the trigger system, amplitude variations, and slight timing misalignments can be caused between post-silicon and pre-silicon data. These non-ideal factors impact the EM map's accuracy, but the resulting MtD values remain within acceptable limits for side-channel evaluation. Therefore, these experimental results affirm the proficiency of EMSIM+GAN in simulating the EM distribution of a real chip based on the cell current and grid information at the layout level, effectively capturing differences between pre-silicon simulation and post-silicon measurements.

VI. EMSIM+GAN+TL VS THE LATEST METHOD

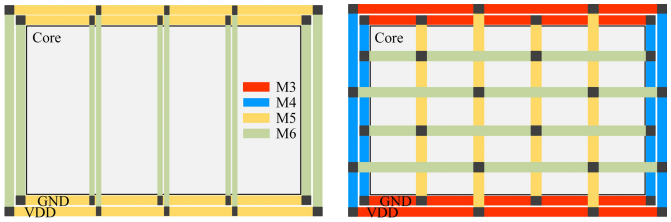
The generalization ability of EMSIM+GAN+TL across different design spaces and the reliability of security evaluation are demonstrated in this section. We select the AES from Section IV as the benchmark circuit to emulate the actual security chip design flow. We implement different protection schemes for AES and transition to a more advanced technology node. EMSIM+GAN+TL applies TL based on the pre-trained model in Section IV, fine-tuning the model to accommodate design variations before conducting security assessments.

A. Experimental Setup

Table IV lists the key information used for feature extraction in the 4 selected experimental designs. AES_mask_1, AES_mask_2 and AES_pg are physically implemented using SMIC 180 nm CMOS technology, while AES_55nm is implemented using SMIC 55 nm CMOS technology. All designs are operated at a 25 MHz clock frequency and 1.8 V supply voltage. Specific details of the 4 designs are shown below.

TABLE IV
DESIGNS USED IN EXPERIMENT III

Feature / Design	Area (μm^2)	Logical cells	Top metal wires
AES_mask_1	1140 × 840	10360	878
AES_mask_2	960 × 960	15995	408
AES_pg	1140 × 840	14448	1186
AES_55nm	346 × 346	14543	5510



(a) AES (b) AES_pg

Fig. 13. Power grids of AES and AES_pg.

1) AES_mask_1: This implementation draws inspiration from the renowned classical masking scheme proposed by Oswald et al. [21]. It uses a combination of additive and multiplicative masks to achieve first-order SCA protection on the AES algorithm.

2) AES_mask_2: The implementation improves the Rotating S-box Mask (RSM) and proposes a cyclic shift random mask scheme based on the tower domain [22], that operates directly on the S-box after the addition of the mask, saving hardware overhead and resource consumption.

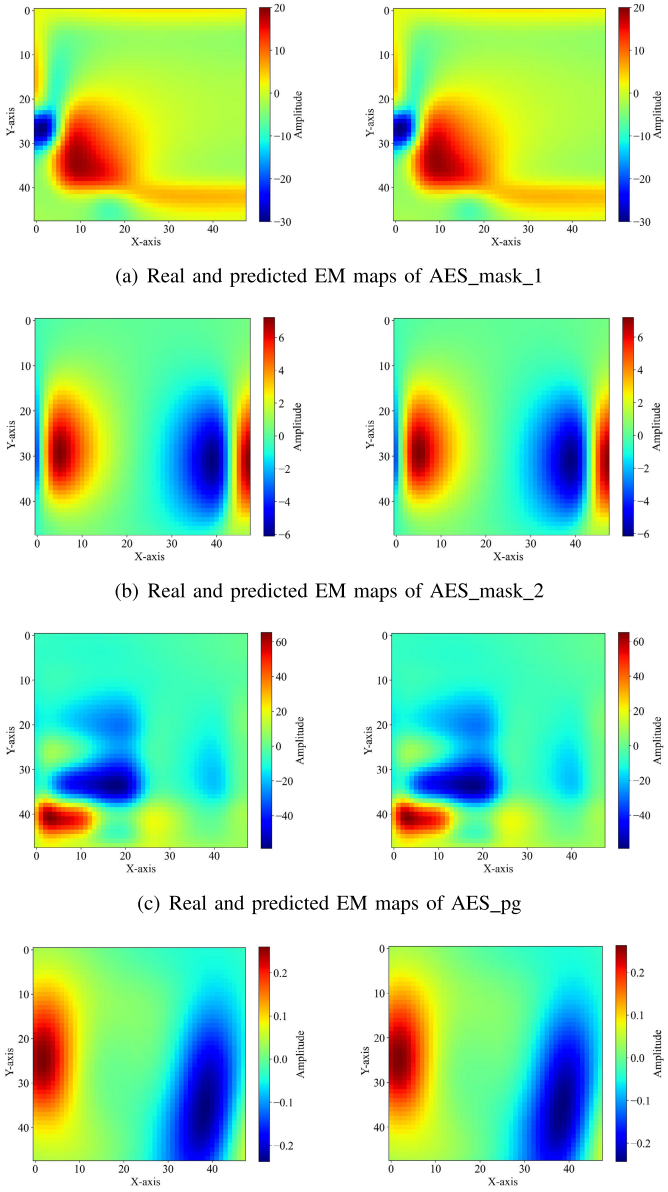
3) AES_pg: This implementation uses a physical protection strategy [23]. Based on the AES benchmark, two sets of vertical power strips are added to the M5 layer and two sets of horizontal power strips are added to the M6 layer. These power strips are uniformly distributed with 40µm width. A comparison of the power grid for AES and AES_pg is shown in Figure 13.

4) AES_55nm: This is an AES benchmark design implemented using SMIC 55 nm CMOS technology.

Our experiments are built on the assumption that the designer initially trained an EMSIM+GAN model to generate EM data for security evaluation following the completion of an initial AES design. Upon identifying a security vulnerability, the designer introduces protection schemes or opts to replace the process node, followed by a reevaluation. To reduce the time required for generating a new model, EMSIM+GAN+TL treats the modified design as a target task (T_t) and uses only 500 sample pairs to fine-tune the existing EMSIM+GAN model. For the evaluation, we also prepare cell current and power grid maps for the EMSIM+GAN+TL flow. The fine-tuned GAN model is then employed to predict EM data for security evaluation.

B. EM Security Evaluation Results

1) EM Emanations and Accuracy Analysis: Figure 14 compares the EM maps of four designs and the EM maps predicted by EMSIM+GAN+TL at a specific point in time. Table V



(a) Real and predicted EM maps of AES_mask_1

(b) Real and predicted EM maps of AES_mask_2

(c) Real and predicted EM maps of AES_pg

(d) Real and predicted EM maps of AES_55nm

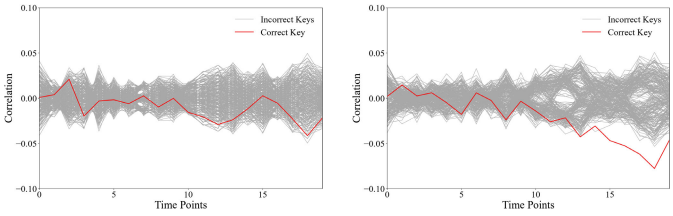
Fig. 14. EM map prediction results from EMSIM and EMSIM+GAN+TL.

summarizes the accuracy performance of EMSIM+GAN+TL for the above designs. Notably, the EM maps generated by EMSIM+GAN+TL achieve NCC and SSIM values exceeding 99.5%. These experimental results demonstrate that EMSIM+GAN+TL effectively improves the performance of T_t, attaining the desired accuracy by transferring the experiences of T_s within the relevant domain. These high accuracy results underscore the versatility and adaptability of the proposed EMSIM+GAN+TL for tasks spanning various design and technology nodes.

2) Security Evaluation of AES_mask_1: Initially, We investigate the first-order security of AES_mask_1. According to Security Level III, we use EMSIM+GAN+TL to generate 10 K EM traces to analyze the potential security vulnerabilities of AES_mask_1. To accomplish this, we construct the HW matrix as an information leakage model by targeting

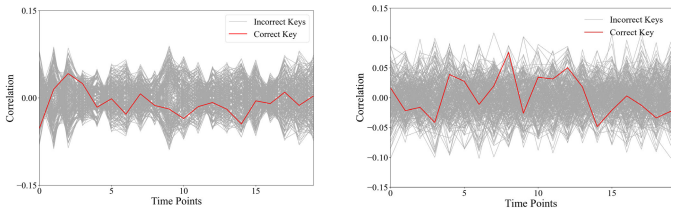
TABLE V
ACCURACY PERFORMANCE OF EMSIM+GAN+TL

Metric \ Design	AES_mask_1	AES_mask_2	AES_pg	AES_55nm
Generator loss	3.9909e-04	2.4904e-04	1.8881e-04	3.2918e-04
NCC	99.9%	99.9%	99.9%	99.9%
SSIM of EM map	99.5%	99.8%	99.9%	99.5%



(a) HW model (b) Toggle-count model

Fig. 15. EM leakage evaluation results of AES_mask_1.



(a) AES_mask_2 (b) AES_pg

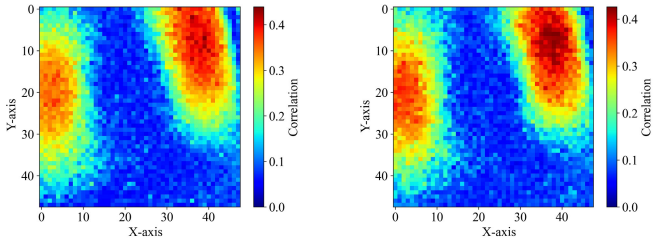
Fig. 16. EM leakage evaluation results of AES_mask_2 and AES_pg.

the registers of the S-Box module. CEMA is carried out on AES_mask_1 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 results of the EM leakage evaluation are shown in Figure 15 (a), affirming the robustness of the masking scheme in preserving the integrity of the correct key.

Nevertheless, is the design really secure? Or is the key unbreakable because the data predicted by EMSIM+GAN+TL lacks the side-channel information associated with the plaintext and the key? To investigate 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 results in Figure 15 (b) demonstrate that 10 K traces are sufficient to reveal the correct key. Therefore, the above analysis results demonstrate that EM data predicted by EMSIM+GAN+TL can be used to evaluate the effectiveness of protection schemes effectively and can diagnose potential security vulnerabilities in circuits.

3) Security Evaluation of AES_mask_2: To further enhance the protection of AES circuits against CEMA attacks, AES_mask_2 employs new protective scheme. The analysis method is consistent with that of AES_mask_1. The results of the EM leakage evaluation are shown in Figure 16 (a), where the correct key is safeguarded by masking operations. This demonstrates the efficacy of tower domain-based cyclic shift random masking as a protective measure.

4) Security Evaluation of AES_pg: Next, we measure the robustness of the power grid-based physical protection strategy against SCA. The CEMA results for 10 K EM traces under the HD model are depicted in Figure 16 (b), showcasing the high resistance of AES_pg to SCA. In practical security chip design and manufacturing, EMSIM+GAN+TL allows designers to iteratively redesign power grids and efficiently evaluate chip security until meeting the desired security requirements.



(a) EMSIM (b) EMSIM+GAN+TL

Fig. 17. EM leakage evaluation results of AES_55nm.

5) Security Evaluation of AES_55nm: Finally, Figure 17 displays the CEMA results of AES_55nm under the HD model. The comparison of the leakage maps generated from EMSIM and EMSIM+GAN+TL demonstrates that EMSIM+GAN+TL can overcome the technology node-specific limitations, enabling fast transfer across different process nodes.

C. Evaluation Efficiency Analysis

The advantage of EMSIM+GAN+TL over the EMSIM+GAN lies in its ability to significantly reduce the time required to acquire a new model from scratch by leveraging prior knowledge. Once the model is trained, the prediction speed of EMSIM+GAN and EMSIM+GAN+TL is practically the same. In fact, the number of samples needed for training the EMSIM+GAN and EMSIM+GAN+TL models differs, primarily due to variations in sample designs and the differences between the new and previous design versions (e.g., process node changes, design modifications, etc.).

In this study, the training dataset for TL is reduced to 500 sample pairs, resulting in approximately half the training time for EMSIM+GAN+TL compared to EMSIM+GAN. Additionally, we modify the sample size from 1000 to 500 in the Equation (9) and (10) to compare the execution times of EMSIM and EMSIM+GAN+TL.

We assume that when using EMSIM+GAN+TL for security evaluation, there exists a pre-trained GAN model adapted to T_s. The execution times and time ratio T_{ratio} of EMSIM and EMSIM+GAN+TL across different circuits and data volumes (ranging from 1 K to 1 M traces) are displayed in Figure 18. It is evident that building upon the base model of the T_s, EMSIM+GAN+TL begins to demonstrate its advantages starting from a measured data volume of around 1 K, with efficiency improvements ranging from 1.89 $\sim$ 1.94 times. Specifically, for the 10 K and 100 K traces corresponding to security level III and IV in ISO/IEC 17825-2016, EMSIM+GAN+TL demonstrates a substantial enhancement in efficiency, exhibiting improvements by factors of 14.22 $\sim$

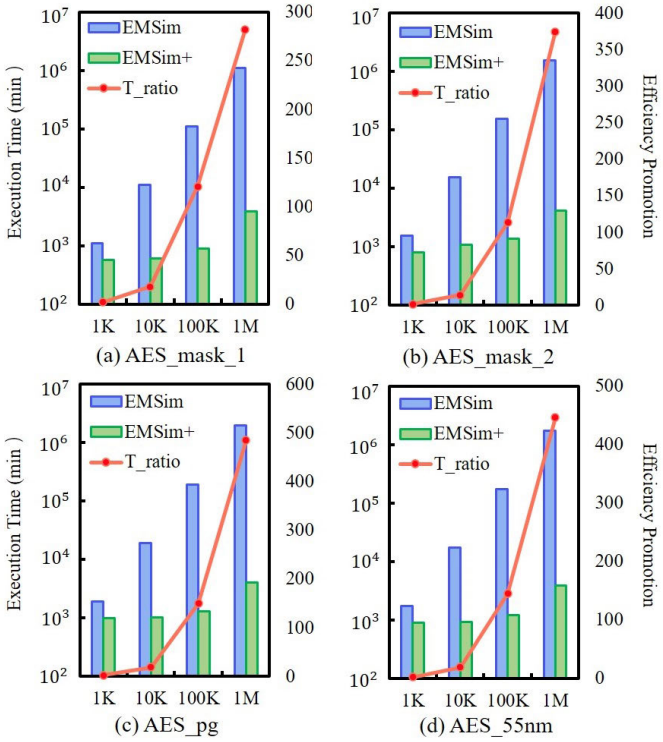


Fig. 18. Efficiency comparison between EMSIM and EMSIM+GAN+TL across different circuits and number of traces.

18.85 times and 113.37 ∼ 149.23 times for each dataset. Furthermore, when assessing 1 M traces, the time efficiency of the evaluation is expected to increase by 282.04 ∼ 483.98 times.

VII. Conclusion and Future Works

In this paper, we develop a novel framework named EMSIM+ for fast pre-silicon EM leakage evaluation. The key idea of EMSIM+ is to introduce ML into the EM security evaluation domain and propose two evaluation frameworks, EMSIM+GAN and EMSIM+GAN+TL. EMSIM+GAN leverages GAN to learn the transient mappings from layout-level cell current data and power grid data to EM data, mitigating the efficiency challenges of traditional simulators in single security evaluations. EMSIM+GAN+TL integrates the TL methodology to significantly reduce the number of samples needed to train GAN models for new designs, allowing EMSIM+'s swift adaptation across different designs and technology nodes. Experimental results show that EMSIM+ can provide fast and accurate feedback at the secure chip design stage with more than ∼ 242× efficiency improvement over state-of-the-art methods.

In future work, we will investigate more intelligent current decomposition schemes to address potential errors caused by the assumption of uniform distribution, compensating for current imbalances. Additionally, we will systematically examine the relationship between chip size and resolution selection to avoid model imbalance arising from significant variations in chip size. This will be achieved by employing adaptive pooling layer structures or leveraging transfer learning.

References

[1] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proc. Annu. Int. Cryptol. Conf.* Santa Barbara, CA, USA: Springer, 1999, pp. 388–397.

[2] Y. Zhao et al., "Side channel security oriented evaluation and protection on hardware implementations of kyber," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 70, no. 12, pp. 5025–5035, Dec. 2023.

[3] K. Monta et al., "Silicon-correlated simulation methodology of EM side-channel leakage analysis," *ACM J. Emerg. Technol. Comput. Syst.*, vol. 19, no. 1, pp. 1–23, Jan. 2023.

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

[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 *Proc. 28th Asia South Pacific Design Autom. Conf. (ASP-DAC)*, Jan. 2023, pp. 670–675.

[6] H. Li, A. T. Markettos, and S. Moore, "Security evaluation against electromagnetic analysis at design time," in *Proc. 10th IEEE Int. High-Level Design Validation Test Workshop*, Nov. 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 *Proc. Int. Workshop Power Timing Modeling, Optim. 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 *Proc. IEEE/ACM Int. Conf. Comput.-Aided Design (ICCAD)*, Nov. 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 Trans. Inf. Forensics Security*, vol. 18, pp. 1365–1379, 2023.

[10] 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 *Proc. 25th Asia South Pacific Design Autom. Conf. (ASP-DAC)*, Jan. 2020, pp. 26–31.

[11] 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 *Proc. IEEE/ACM Int. Conf. Comput.-Aided Design (ICCAD)*, Nov. 2019, pp. 1–8.

[12] 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 *Proc. 26th Asia South Pacific Design Autom. Conf. (ASP-DAC)*, Jan. 2021, pp. 690–696.

[13] I. J. Goodfellow et al., "Generative adversarial networks," *Commun. ACM*, vol. 63, no. 11, pp. 139–144, 2020.

[14] K. Weiss, T. M. Khoshgoftaar, and D. Wang, "A survey of transfer learning," *J. Big Data*, vol. 3, no. 1, pp. 1–40, May 2016.

[15] G. Singha, D. Diamantopoulosb, J. Gómez-Lunaa, S. Stuijkc, H. Corporaalc, and O. Mutlua, "LEAPER: Fast and accurate FPGA-based system performance prediction via transfer learning," in *Proc. IEEE 40th Int. Conf. Comput. Design (ICCD)*, Oct. 2022, pp. 499–508.

[16] J. Kwon and L. P. Carloni, "Transfer learning for design-space exploration with high-level synthesis," in *Proc. ACM/IEEE 2nd Workshop Mach. Learn. CAD (MLCAD)*, Nov. 2020, pp. 163–168.

[17] Y. Lin et al., "Data efficient lithography modeling with transfer learning and active data selection," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 38, no. 10, pp. 1900–1913, Oct. 2019.

[18] T. Gai et al., "Flexible hotspot detection based on fully convolutional network with transfer learning," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 41, no. 11, pp. 4626–4638, Nov. 2022.

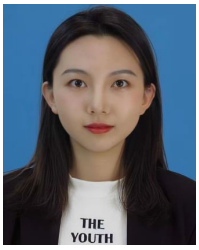
[19] Y. Wang and M. Tang, "A survey of side-channel leakage assessment," *Electronics*, vol. 12, no. 16, p. 3461, Aug. 2023.

[20] 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.

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

[22] Y. Yan, J. Wang, and Y. Liu, "Design method of generic cyclic shift mask based on tower field," *J. Electron. Inf. Technol.*, vol. 43, no. 9, pp. 2489–2497, 2021.

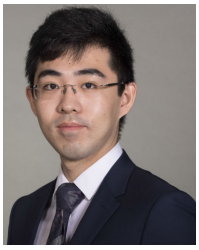
[23] M. Wang et al., "Physical design strategies for mitigating fine-grained electromagnetic side-channel attacks," in *Proc. IEEE Custom Integr. Circuits Conf. (CICC)*, Apr. 2021, pp. 1–2.



Ya Gao received the B.S. degree in electronic science and technology from Tianjin University, Tianjin, China, in 2020, where she is currently pursuing the Ph.D. degree with the School of Microelectronics. Her current research interests include hardware security, EDA tools, and machine learning.

Haocheng Ma received the B.S. degree in microelectronics from Tianjin University, Tianjin, China, in 2017, and the Ph.D. degree from the School of Microelectronics, Tianjin University, in 2023. His current research interests include digital circuit design, hardware security, and EDA for security.

Qizhi Zhang received the B.S. degree in microelectronics from Tianjin University, Tianjin, China, in 2019, where he is currently pursuing the Ph.D. degree in microelectronics and solid state electronics with the School of Microelectronics. His current research interests include digital circuit design, hardware security, and formal verification.



Xintong Song received the master's degree in chemical engineering from Georgia Institute of Technology in 2017 and the master's degree in computer engineering from New York University in 2020. He is currently pursuing the Ph.D. degree with the School of Microelectronics, Tianjin University. He was a System Software Engineer with Sina Corporation. His research interests include fully homomorphic encryption (FHE), post-quantum cryptography (PQC), and cryptography software and hardware co-design and optimization techniques.

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), and also a Professor with the School of Cyber Science and Technology, University of Science and Technology of China. His research focuses on the areas of 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.

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

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

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