# EO-Shield: A Shield-Based Protection Scheme Against Both Invasive and Non-Invasive Attacks

Ya Gao, Qizhi Zhang, Xintong Song, Haocheng Ma, Jiaji He, and Yiqiang Zhao

***Abstract*— Smart devices, especially Internet-connected devices, typically incorporate security protocols and cryptographic algorithms to ensure the control flow integrity and information security. However, various types of attacks try to tamper with these devices, including invasive and non-invasive. Chip-level shields have been proven effective against invasive attacks, but the potential of shields as a protection mechanism against side-channel analysis (SCA) attacks remains under-explored. To bridge this gap, we propose a shield-based multi-functional protection scheme, named EO-Shield, capable of simultaneously thwarting invasive and non-invasive attacks. EO-Shield is implemented using the chip's top metal layer and includes an Information Leakage Obfuscation Module (ILOM) underneath. This module generates its protection patterns based on the operating conditions of the circuit that need to be protected, thus reducing the correlation between electromagnetic (EM) emanations and cryptographic data. Additionally, we introduce a simulation technique to test the protection efficacy of EO-Shield at the layout level, utilizing commercial Electronic Design Automation (EDA) tools and the EMSIM/EMSIM+ tool. Simulation experiments demonstrate that the ILOM decreases the signal-to-noise (SNR) ratio to below 0.6 and improves the difficulty of SCA attacks by more than 100 times. Compared to existing single-function protection methods against physical attacks, EO-Shield leverages the EM protection potential of shields to offer multi-functional protection.**

***Index Terms*— Active shield, invasive attack, electromagnetic side-channel security.**

## I. INTRODUCTION

INTEGRATED circuits (ICs) have been widely used in various information infrastructures, including electronic payment, Internet of Things (IoT), 5G mobile communications, etc. These infrastructures often rely on embedded devices that incorporate cryptographic algorithms to protect the confidentiality, authenticity, and integrity of sensitive data. Despite their importance, ICs are not immune to security threats. For instance, attackers have successfully used power side-channel analysis (SCA) attacks to recover the global AES-CCM key used by Philips Hue's smart lighting system to encrypt and authenticate new firmware updates. This highlights the need for improved security measures to protect ICs and the sensitive data they handle [1].

State-of-the-art physical attacks can be generally categorized as invasive and non-invasive attacks [2]. Invasive attacks involve direct manipulation of the device's physical components, while non-invasive attacks exploit the devices' various physical characteristics to extract sensitive information. A focused ion beam (FIB) attack is one of the most extensively studied invasive attacks. Once the chip is depackaged, the FIB attack can directly manipulate the connections of the metal nets and access confidential data from the chip, posing a significant threat [3]. Non-invasive attacks are dominated by SCA attacks. SCA attacks aim to extract sensitive information from the chip by collecting and analyzing various physical parameters of the chip. These exploitable parameters include electromagnetic (EM) emanation, power consumption, timing variations, etc [4]. Compared to other side-channel parameters, EM does not necessitate direct connections to the chip and can obtain local EM information with a high signal-to-noise ratio (SNR). Thus, EM information emitted by the chip has gradually attracted much research interest recently due to these advantages above [5].

To counter invasive attacks, several countermeasures have been proposed in the form of analog sensors [6], $t$-private circuits [7] and shields [8], [9]. Notably, the reliability of analog sensors can be affected by advanced technology nodes, and the transformation of $t$-private circuits incurs substantial area overhead. Shield-based solutions are so far the most common countermeasure, primarily implemented using the top metal layer of the chip [10], [11]. There are currently two types of shields, passive and active. Passive shields detect whether the shield has been damaged by attacks such as cutting by recognizing changes in capacitance [12]. Active shields proactively detect FIB attacks in real-time by monitoring specific dynamic signal sequences inside the shield network [13]. To enhance a chip's resistance to SCA attacks, it is common to use noise injection (NI) and correlation signature suppression to reduce the SNR from the chip's physical implementation point of view [14]. Some representative protection methods include wave dynamic differential logic (WDDL) [15], dual-rail pre-charge (DRP) circuits [16], sense amplifier-based logic (SABL) [17], etc. However, existing physical protection methods could introduce $> \sim 2\times$ overall overheads.

To the best of our knowledge, no multi-purpose protection method exists that can effectively counter both invasive

Manuscript received 10 April 2024; revised 4 June 2024; accepted 17 June 2024. Date of publication 3 July 2024; date of current version 30 January 2025. This article was recommended by Associate Editor Q. Liu. *(Corresponding authors: Jiaji He; Yiqiang Zhao.)*

The authors are with the School of Microelectronics, Tianjin University, Tianjin 300072, China (e-mail: gaoyaya@tju.edu.cn; qizhi_zhang@tju.edu.cn; xintong_song@tju.edu.cn; hc_ma@tju.edu.cn; dochejj@tju.edu.cn; yq_zhao@tju.edu.cn).

Digital Object Identifier 10.1109/TCSI.2024.3418777

and non-invasive attacks simultaneously. Notably, it has been demonstrated that shields can attenuate EM emanations from internal circuits, thus providing some level of SCA protection. Experimental results by Ngo et al. showed that attacking an AES circuit protected by a shield requires 5000 additional EM traces compared to an unprotected circuit [18]. The authors proved that activating the shield's protection scheme increases the difficulty of SCA attacks. However, they didn't perform a theoretical analysis or design specialized stimuli for the active shield to achieve complete SCA protection. Katz et al. demonstrated through theoretical studies and simulation experiments that the active monitoring by existing shields introduces additional noise to the chip's EM emanations, which can mitigate the information leakage [19]. However, the authors did not provide SCA attack results on cryptographic chips, leaving the effectiveness of introducing random signals into the shield to counter SCA attacks unproven. Miki et al. used a backside buried metal structure to form a shield on the Si-backside that is capable of detecting physical backside attacks against the chip and can protect the circuit from power-side channel attacks [10].

By properly utilizing the newly introduced random noise, it's possible to lower the EM side channel's SNR and increase the complexity of SCA attacks. In this paper, we propose and implement Electromagnetic Obfuscation Shield (EO-Shield), which is a multi-functional protection scheme against both FIB and SCA attacks. Based on our prior work involving active shields [20], we further exploit the noise introduced by the monitoring activities of the active shields to fortify defenses against EM SCA attacks. The signals fed into the shield's wire mesh are meticulously generated based on the chip's behaviors to obfuscate the chip's EM emanations. This signal generation module is integrated underneath the active shield. Once EM emanations of the chip and the active shield are superimposed in space, the original EM emanations from the chip become hidden within the overall superimposed EM emanations. To visualize the effect of layout-level EM emanations under EO-Shield, we use a combination of commercial Electronic Design Automation (EDA) tools and EMSIM [21] or EMSIM+ [22] tool for the EM simulation of active shields and evaluate the protection effect of EO-Shield. TABLE I provides a summary of the existing works on a shield as a countermeasure to EM SCA attack and presents our work for comparison. More specifically, our work makes the following contributions:

- A shield-based multi-functional protection scheme named EO-Shield is proposed to counter both invasive and non-invasive attacks. EO-Shield utilizes a top metal layer to implement an active shield that monitors FIB attacks and proactively obfuscates EM emanations.
- EO-Shield contains an Information Leakage Obfuscation Module (ILOM) to provide stimuli based on the behavior of the underlying circuit. These stimuli are supplied directly to the active shield that obfuscates the EM emanations of the circuit.
- We construct an EM simulation framework adapted to the active shield. The current stimuli through the active shield and the layout parasitic parameters are extracted using commercial EDA tools. Then we choose EMSIM/EMSIM+ tool for EM calculations.
- Three exemplary cryptographic circuits are developed using EO-Shield scheme. Through simulating EM emanations of the circuits with and without EO-shield and performing security evaluations, the effectiveness of EO-Shield against SCA attacks is proved.

The rest of this paper is organized as follows. Section II introduces the background of invasive attacks and EM SCA attacks. Then, the details of our proposed EO-Shield are shown in Section III. Section IV demonstrates the effectiveness of EO-Shield on 3 exemplary cryptographic circuits. Section V and Section VI shows the effect of EO-Shield with different shield topologies and clock frequencies, respectively. We also measure the overhead of EO-Shield in Section VII. Future work and Conclusions are drawn in Section VIII and Section IX.

## II. BACKGROUND

### A. Invasive Attacks

The invasive attack is an important method of cracking chips, typically using FIB devices to obtain critical chip information via reverse engineering, micro-probing, and other destructive methods. FIB serves as a powerful circuit editing tool capable of precisely milling and depositing material on silicon dies, making it simple to cut, connect, and alter the chip's metal alignment [23]. A typical invasive attack is carried out using a FIB workstation and consists of the following four steps [24]:

1) ***Reverse engineering:***
This is the first step in most invasive attacks. Once the chip is decapsulated, the attacker gains insights into the chip's circuit architecture and design. Subsequently, the layout and netlist are extracted to pinpoint areas vulnerable to attack. For cryptographic chips, one of the most important tasks in the reverse engineering step is identifying the asset nets, such as encryption keys.
2) ***Locating the target wire:***
The position of the target wire can be ascertained through a one-to-one mapping between the netlist and the layout. This also enables the determination of whether severing the metal wire will impact the extraction of the target wire. Modern tools, such as Chipworks' ICWorks, offer automated netlist extraction from images of each layer captured with optical or scanning electron microscopes, significantly streamlining the attacker's workload.
3) ***Probing pad creating:***
Creating a conductive path for probing needs to be established while maintaining the integrity of the remaining circuitry on the chip. It entails precisely milling a hole to reveal the target wire, depositing metal onto it, and subsequently extracting the key signal while forming a metal cross pad with FIB devices. This step requires a precise-enough kinematic mount, and fiducial markers to base the coordinates.

TABLE I
COMPARISON OF CURRENT WORKS ON SHIELDS AS COUNTERMEASURES TO EM SCA ATTACK

| Work | Shield Type | Coverage | Measurement | Counter EM SCA |
|---|---|---|---|---|
| [18] | Active | Front-side | Real measurements | Random bit, no specifically designed protective circuit |
| [19] | Active | Front-side | Simulation | Random bit, no SCA results |
| [10] | Active | Back-side | Real measurements | None, but demonstrates power decay |
| Ours | Active | Front-side | Simulation | Specifically designed protective circuit and SCA results |

4) ***Extracting target information:***
Finally, The target signal is probed using a probe table staked to the metal pad.

Among the four steps outlined, reverse engineering poses the greatest challenge. This process involves utilizing chemical expertise to properly decapsulate the chip, remove copper plates from its backside, and subsequently reconstruct each layer through microscopic imaging. As a result, sophisticated shields have emerged as the primary method for thwarting invasive attacks. Constructed with a top metal layer, these shields not only create a robust physical barrier against attackers but can also be equipped with sensing units. These units are designed to identify attacks originating from the metal layer positioned at the front of the device.

### *B. EM Side-Channel Analysis Attacks*

Side channel analysis (SCA) attacks were first demonstrated by Kocher et al. in 1998 using simple power analysis (SPA) and differential power analysis (DPA) [25]. As new attack vectors emerged, Quisquater and Samyde expanded the scope of SCA in 2001 by introducing simple EM analysis (SEMA) and differential EM analysis (DEMA), marking the entry of EM SCA into the field of side-channel attacks [26]. Meanwhile, Gandolfi et al. carried out real-world EM side-channel attacks on three chips using different cryptographic algorithms and hardware protection measures [27]. In 2004, Brier et al. highlighted the shortcomings of previous methods such as DPA and then introduced correlation power analysis (CPA) [28]. Over the past decade or so, a great deal of SCA research has focused on cryptographic modules as a primary target, causing a significant security concern for various cryptographic algorithms (AES, DES, RSA, PRESENT, etc.) implemented on electronic devices.

During the operation of cryptographic chips, due to the current accumulation and the metal shielding effects [21], the currents flowing in the interconnect wires will converge within the top metal layer, resulting in the top metal layer carrying strong EM emanations. EM SCA leverages a near-field probe coupled to the magnetic field of the chip to collect EM emanations and steal the secret key by analyzing the correlation between the input (or output) data, the secret key, and the EM data. Among the EM SCA techniques, correlation EM analysis (CEMA) is the most widely used. CEMA utilizes Pearson's correlation as a statistical method to recover keys by correlating the measured EM side-channel traces with sensitive intermediate values. For our analysis, we assume a passive attacker who lacks knowledge of the sensitive information within the victim chip, but has physical access to it, enabling the acquisition of EM side-channel information. Fig. 1 illustrates how CEMA works in the following steps:

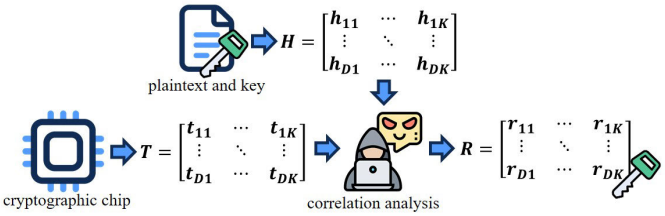



Fig. 1. Traditional CEMA process.

1) ***Select the intermediate value value:***
For the encryption algorithm, the chosen intermediate value should satisfy the function $f(d, k)$, where $d$ is usually the plaintext and $k$ is part of the key.
2) ***Collect the EM traces:***
Use the near-field coupling technique to acquire non-invasive information between the probe and the chip under test. Collect the EM traces generated during $D$ times encryption to obtain the EM information leakage matrix $T$.
3) ***Calculate the hypothetical EM information leakage matrix:***
The Hamming distance (HD) or Hamming weight (HW) model is used to generate a hypothetical EM information leakage matrix $H$ based on the guessed key values and known plaintext.
4) ***Correlation Analysis:***
The correlation between the matrices $T$ and $H$ is calculated using Equation (1) below to yield the correlation matrix $R$, where the guessed key with the highest correlation is the true key.

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

Notably, CEMA is not only an attack method but also an attacking-style assessment method used for security assessment of cryptographic chips [29]. Another assessment method used for cryptographic chip security certification standards is the leakage detection-based method, known as Test Vector Leakage Assessment (TVLA). Compared with TVLA, CEMA is not susceptible to false positives or false negatives. This accuracy allows evaluators to directly identify potential security vulnerabilities, offering a comprehensive assessment of

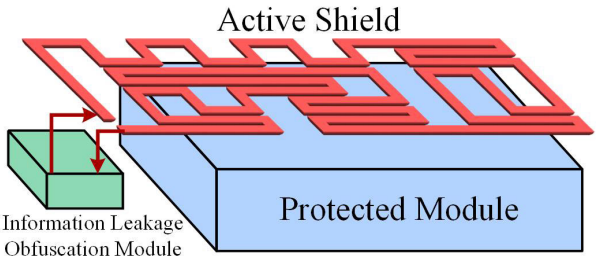



Fig. 2. The architectural of the proposed EO-Shield.

cryptographic chips and aiding in the design of protection measures.

## III. EO-Shield System Design and Simulation Methodology

The proposed EO-Shield protection scheme framework is illustrated in Fig. 2, consisting of an active shield and an Information Leakage Obfuscation Module (ILOM). In our framework, the active shield is meticulously designed to cover the protected region of the chip. Simultaneously, the ILOM is configured to monitor invasive attacks and generate signals that induce additional EM emanations within the wire mesh. More specifically, when an invasive attack happens, such as tampering with the active shield by cutting or shorting it, the ILOM activates an alert signal. Furthermore, the signals motivated into the wire mesh can obfuscate the EM side-channel information, thereby enhancing resistance against SCA attacks.

### A. Random Active Shield Design and Implementation

To effectively counter invasive attacks such as probing and FIB, the active shield needs to satisfy three basic principles, connectivity, full coverage, and complexity. Connectivity allows detection circuits to identify the shield's damage in real time, subsequently activating an alarm or a protective mechanism. Full coverage means that the protected area of the circuit is completely covered under the shield. Complexity requires that the shield's topology exhibit a high entropy value, a concept introduced by Briais et al. to quantify the shield's complexity [30]. An entropy value approaching 1 signifies the routing pattern of the shield is highly randomized, which increases the difficulty for attackers attempting to decipher or disrupt the shield's integrity.

Existing active shield designs encompass configurations like serpentine, parallel, Hilbert curve, Peano curve, and the random Hamiltonian topology. Among these options, the random Hamiltonian topology offers the highest entropy value, allowing it exceptionally resilient against invasive attacks. In the context of our proposed EO-Shield system, we use an available algorithm for active shield generation. Based on our previous work, we use the shield generation software to produce active shields with random Hamiltonian topology. This is executed through the utilization of an innovative algorithm known as the Artificial Fish-Swarm Random Hamiltonian algorithm (AFSRHA) [31].

Fig. 3 provides an overview of the AFSRHA execution process. The dimensions of the shield area are designated as $L$ for length and $W$ for width, respectively. The wire width and wire space of wire mesh are also specified by *wire_width* and *wire_space*. $L$ and $W$ are normalized into grid points by *wire_width* and *wire_space*. A square area formed by four adjacent grid points is defined as a fish. A fish is randomly selected and then merged with an adjacent fish to generate loop C. Subsequently, a fish adjacent to loop C is randomly selected and merged into loop C. This process is iterated until all the fish have been incorporated into loop C, signifying the completion of the active shield generation.

The AFSRHA algorithm requires that $L$ and $W$ satisfy:

$$L, W \geq 8 \times (wire\_width + wire\_space) \tag{2}$$

When $L$ or $W$ does not satisfy Equation (2), for example, the shield area is the gap between the dense power strips on the top layer. We encounter a narrow, elongated shield area scenario. To address this, we introduce the concept of a random parallel shield topology for the first time. As shown in Fig. 4, this random parallel shield topology generates an active shield with a good protective effect by randomly selecting the offset in the x-direction and y-direction during the generation process.

### B. Information Leakage Obfuscation Module (ILOM) Design

The ILOM, illustrated in Fig. 5, includes five principal components: the Linear Feedback Shift Register (LFSR), the RO generator, the multiplexer (MUX), the Frequency Divider, and the Comparison Module. This module is meticulously designed to consider both the potential attackers' strategies and the implementation of the protected cryptographic circuits. Its primary function is to produce noise during cryptographic operations, which, in turn, induce EM emanations through the active shield, thereby masking the EM emanations of the underlying protected circuit through the NI mechanism. In the context of SCA attacks, attackers typically focus on the moment when key-related operations occur. Because the flip-flops hold the critical data emit significant EM information during state transitions, which points of interest for attackers. Typically, these state changes in flip-flops occur after the clock's rising or falling edges. Therefore, we divide the clock cycle of the underlying cryptographic circuit into two parts. During the segment corresponding to flip-flop activity, a high-frequency RO signal ($RO\_out$) is sent to the shield, thereby ensuring that any collected EM information by attackers is effectively obfuscated. During the other half cycle, a random 1-bit signal ($lfsr\_out[9]$) generated by the LFSR is sent to the shield. This signal assists the Comparison Module in determining whether an attack on the shield is in progress. The components of the ILOM are described in detail as follows:

***1) LFSR*** is a commonly used method for generating pseudo-random numbers based on Primitive Polynomials. It consists of several D flip-flops and XOR gates. The random signal generated by LFSR will be motivated into the active shield. In practice, the primitive polynomials can be chosen according to specific stochasticity requirements. For example, a 15-bit LFSR can utilize Equation 3 to achieve the maximum

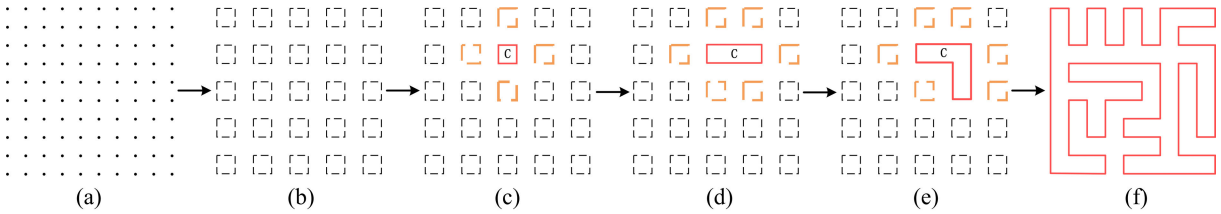



Fig. 3. The execution process of AFSRHA algorithm.

Fig. 4. The structure of a random parallel shield.

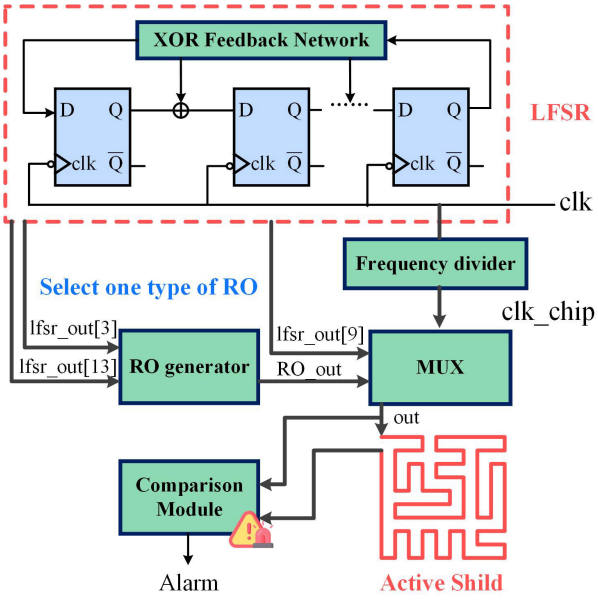



Fig. 5. The structure of the ILOM.

number of output states.

$$x^{15} + x + 1 \tag{3}$$

***2) RO generator*** is employed to produce EM noise that obfuscates the EM emanations generated during the operations of the protected circuits. Given that the time delay in the RO oscillator is directly proportional to the number of inverters, our RO generator includes 4 oscillator circuits with 3, 5, 7, and 9 inverters, respectively. Each configuration demonstrates progressively extended time delays. The inputs for the RO generator are sourced from two LFSR signals, $lfsr\_out[3]$ and $lfsr\_out[13]$. These two random signals can generate four unique combinations that are utilized to select the RO signal in four configurations.

***3) The Frequency Divider*** divides the high-frequency clock signal $clk$ of the ILOM into a derived $clk\_chip$ signal, which then serves as the clock of the protected circuit. This process increases the difficulty for attackers to pinpoint the precise timing window for an attack. Assume that the clock period $t_{pro}$ of the protected circuit contains $n$ clock periods $t_{obf}$ of the EM leakage obfuscation module. Based on the principles of pseudo-random number generation, the probability that the generated pseudo-random signal remains unchanged over the duration $t_{pro}$ is $1/2^{n-1}$. Therefore, the clock frequency of the ILOM must be high enough to ensure that there are enough changing pseudo-random signals for signal comparison.

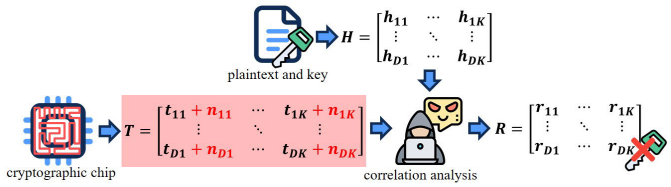



Fig. 6. CEMA process with an EO-Shield.

***4) The MUX*** provides two switching modes for signals input to the active shield, $RO\_out$ or $lfsr\_out[9]$. Depending on the trigger condition of the flip-flop, the MUX switches between the two output modes by detecting the rising or falling edge of the clock $clk\_chip$.

***5) The Comparison Module*** compares the random signals input to the active shield with the signals output from the active shield. This process allows real-time monitoring of invasive attacks and triggers an alarm signal in the event of a mismatch.

Fig. 6 visually outlines the CEMA process when targeting the chip with EO-Shield. Since the active shield is closer to the EM probe and is fed with the signal generated by the ILOM, the actual EM information leakage matrix $T$ measured by attackers also contains the noise magnetic field (i.e. $n_{1,1}, n_{1,2} \ldots\ldots n_{D,T}$) generated by the active shield. Consequently, by correlation analysis with the hypothetical EM information leakage matrix, attackers cannot recover sensitive information.

### C. Simulation Framework for EO-Shield

To develop a framework suitable for the EM simulation of the active shield and to assess the effectiveness of EO-Shield, we establish a simulation flow depicted in Fig. 7. This simulation flow encompasses several key steps: extracting layout parameters using Virtuoso, obtaining Piece-Wise Linear (PWL) current stimuli of ILOM, and executing the EM calculation process through the EMSIM/EMSIM+ tool.

In the parameter extraction process, our framework starts with attaching a resistor to each end of the active shield, labeling them as $VDD$ and $VSS$, respectively. We also assign a label, $Wire$, to the entire metal wire to facilitate the

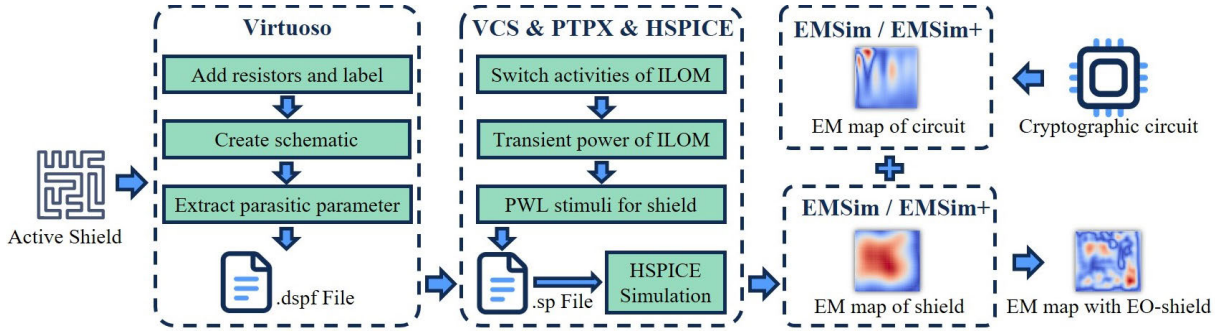



Fig. 7. The simulation framework for EO-Shield.

construction of the shield circuit's schematic. Calibre PEX accepts the layout and schematic for parameter extraction of the shield. We perform transistor-level simulation and store the extracted resistance and capacitance parameters in a.dspf file format.

The signals generated by ILOM will be present in the form of PWL current stimuli in the .sp file for subsequent HSPICE simulations. The current stimuli are extracted by co-simulation of VCS and Primetime PX (PTPX). PTPX solves the dynamic power consumption with a time scale of 1 ns using switch activities of signals extracted by VCS, and the power consumption value divided by the supply voltage yields the transient current.

Finally, with a volume of evaluation data around 1K, we use EMSIM to calculate EM emanations of cryptographic circuits and the active shield (approximately 2282 minutes to generate 1K EM data). EMSIM is a high-precision layout-level chip EM simulator that predicts the EM behavior of circuits based on the physical layout to aid in the pre-silicon quantification and validation of the chip's EM side-channel security. When the data volume continues to increase, we use an advanced version of EMSIM, i.e., EMSIM+ to generate EM maps(approximately 2387 minutes to generate 10K EM data). EMSIM+, based on EMSIM, significantly increases the simulation speed of EM data with the help of a generative adversarial network (GAN) while maintaining accuracy. The entire experiment is implemented on a 6-core CPU computer equipped with NVIDIA GeForce RTX 3090 GPUs.

## IV. Effect of EO-Shield on Different Circuits

To assess the credibility and effectiveness of EO-Shield as a multi-functional protection scheme, we meticulously select 3 exemplary cryptographic circuits implementing conventional encryption algorithm, lightweight encryption algorithm, and processor with instruction set extensions (ISEs). In the first part of the experiments, we conduct a comparative analysis of the circuits, both with and without EO-Shield, focusing on their CEMA results. Our analysis uses Pearson's correlation coefficient and the minimum trace of the disclosed key (MtD) to provide a comprehensive evaluation.

### A. Experimental Setup

All 3 designs chosen for this Section are physically implemented utilizing SMIC 180 nm CMOS technology and run at a 25 MHz clock frequency with 1.8 V supply voltage. Specific design details are displayed in TABLE II. In addition, all designs are realized using 5 metal layers, with the top layer for the active shield. During the encrypted operation, the ILOM starts running at 250 MHz and generates the current stimuli delivered to the active shield.

First, we provide 1K sets of random stimuli for each design and construct their EM simulation models with and without EO-Shield protection using the simulation methodology in Section III-C. Second, we perform the CEMA described in Section II-B for designs without EO-Shield protection. To measure the robustness of EO-Shield against SCA attacks, we further quickly simulate 10K sets of EM data using the EMSIM+ tool. Finally, using the EM data generated by the EMSIM+, we perform CEMA on designs with EO-Shield protection.

### B. Experimental Results of AES_128

Fig. 8 (a) and (b) present the layout of the AES_128 circuit and the structure of the active shield at the top layer, respectively. For AES_128, the byte substitution operation of the S-BOX is a known target for SCA attacks. Therefore, we utilize the EMSIM tool to simulate the EM emanations of the AES_128 during the time of the first-byte substitution operation. The simulation time span is one clock cycle, i.e., 40 ns. Since the time scale of PTPX is 1 ns, one EM trace contains 40 time points. EMSIM partitions the chip surface into $23 \times 17$ grid tiles, constructing an EM map as shown in Fig. 8 (c). Subsequently, we simulate the EM emanations of AES_128 with EO-Shield, generating an EM map shown in Fig. 8 (d) with the same resolution. Note that we only display the EM map at a specific time point where EM emanations are most pronounced for comparison. The results indicate that the integration of EO-Shield modifies the chip's original EM emanations, effectively hiding and transferring the EM hot spots.

Further, we extract EM traces from the hot spots located in the upper right corner of Fig. 8 (c) and illustrate the temporal variation of EM emanations in Fig. 9 (a). The x-axis denotes the simulation time points, while the y-axis represents the EM amplitude. These traces capture the SubByte operation in the first S-Box, where the two prominent peaks correspond to register flips, and the series of lower peaks after $21ns$ are indicative of combinational logic operations. Similarly,

TABLE II
DESIGN USED IN EXPERIMENT

| Design | Specifics | Area ($\mu m^2$) |
|---|---|---|
| AES_128 | Implement the complete AES algorithm designed in compliance with the NIST standard with 128-bit input plaintext and key. | $1140 \times 840$ |
| PRESENT | Implement the S-BOX operation of the PRESENT algorithm with a 80-bit key. | $300 \times 300$ |
| AES_ISEs | Implement ISEs for AES algorithm acceleration based on a 32-bit in-order AES_ISEs processor architecture. | $900 \times 900$ |

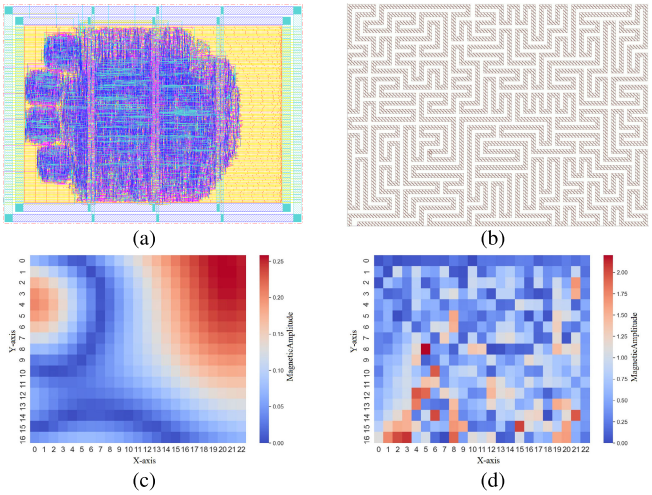



Fig. 8. Chip layout and EM maps of AES_128 without and with EO-Shield. (a) Chip layout of AES_128. (b) Active shield design on the top layer. (c) EM map of AES_128 without EO-Shield. (d) EM map of AES_128 with EO-Shield.

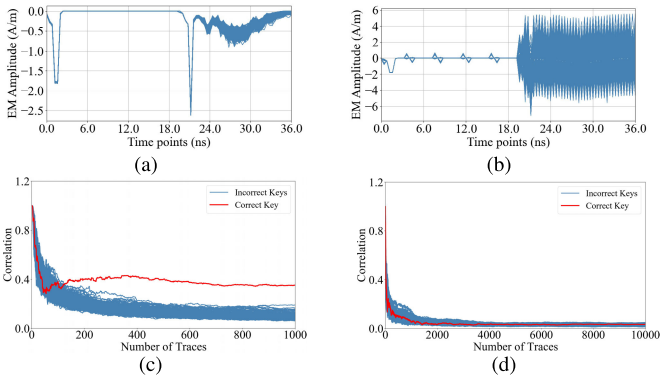



Fig. 9. EM traces and CEMA results of AES_128 without and with EO-Shield. (a) EM traces of AES_128 without EO-Shield. (b) EM traces of AES_128 with EO-Shield. (c) MtD results of AES_128 without EO-Shield. (d) MtD results of AES_128 with EO-Shield.

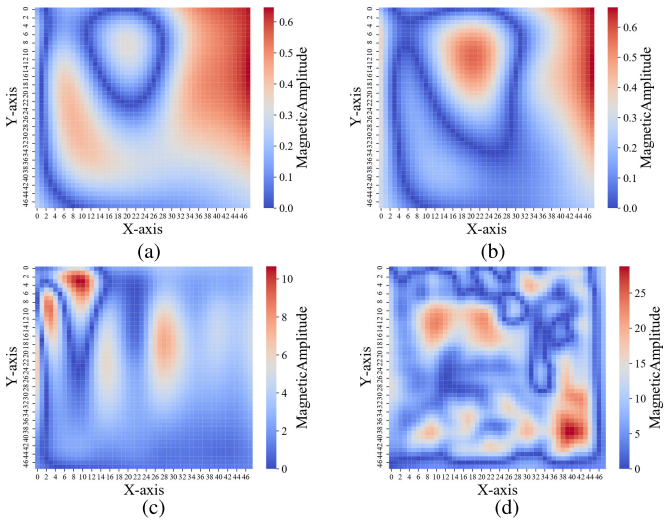



Fig. 10. EM maps of PRESENT and AES_ISEs. (a) EM map of PRESENT without EO-Shield. (b) EM map of PRESENT with EO-Shield. (c) EM map of AES_ISEs without EO-Shield. (d) EM map of AES_ISEs with EO-Shield.

we extract EM traces of AES_128 with EO-Shield at the same location, as depicted in Fig. 9 (b). It can be seen that the EM emanations generated by the circuit encryption process are effectively hidden by the noise produced by the ILOM.

Finally, we build the HD model and traverse all grid tiles in EM maps to perform CEMA on AES_128. Fig. 9 (c) illustrates the CEMA result of AES_128 without EO-Shield, where the x-axis signifies the number of EM traces and the y-axis represents the correlation coefficient. The highest correlation coefficient for the correct hypothetical key exceeds 0.35 and separates from the wrong hypothetical key at the 124-th trace, i.e., MtD = 124. For AES_128 with EO-Shield, we generate 10K traces using the EMSIM+ tool. The corresponding CEMA result in Fig. 9 (d) indicates that the key recovery is unattainable, thereby affirming that EO-Shield provides an effective defense against SCA attacks and enhances security performance.

### C. Experimental Results of PRESENT and AES_ISEs

For the EM simulation of PRESENT and AES_ISEs, EMSIM divides the chip surface into $48 \times 48$ grid tiles and EM simulation results are displayed in Fig. 10. The presence of the EO-Shield leads to a drastic change in EM maps. When performing CEMA, both PRESENT and AES_ISEs focus on registers for byte substitution operations during the first round of encryption. We construct HD and HW models for the two designs, respectively. Without EO-Shield, only 290 and 11 traces are needed respectively to recover the keys of PRESENT and AES_ISEs. To evaluate the protection effect of EO-Shield, we also use the EMSIM+ tool to generate 10K traces. The CEMA results in Fig. 11 show that 10K traces still cannot allow the correct keys of PRESENT and AES_ISEs to be revealed, which proves the excellent protection ability of EO-Shield and the adaptability for different cryptographic circuits.

## V. EFFECT OF EO-SHIELD WITH DIFFERENT TOPOLOGIES

This Section further enriches the scenarios of EO-Shield by evaluating and analyzing shields with various topologies.

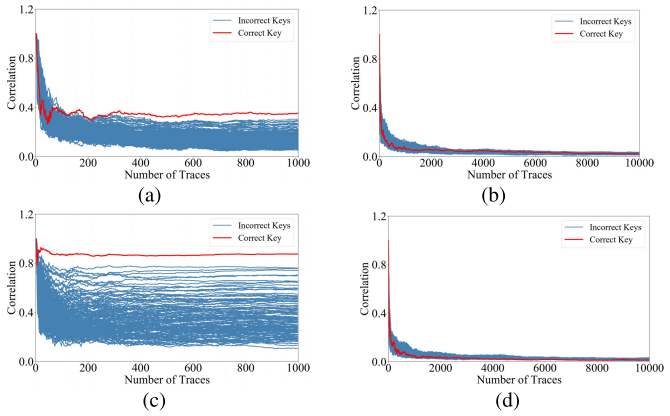



Fig. 11. CEMA results of PRESENT and AES_ISEs. (a) MtD result of PRESENT without EO-Shield. (b) MtD result of PRESENT with EO-Shield. (c) MtD result of AES_ISEs without EO-Shield. (d) MtD result of AES_ISEs with EO-Shield.

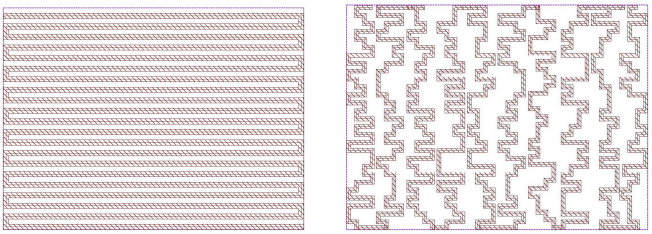



Fig. 12. Different topologies of shields. (a) Parallel topology. (b) Random parallel topology.

Beyond the Hamiltonian topology, we implement two additional shield topologies for EO-Shield: parallel topology and random parallel topology. Then, we compare their protective efficacy against EM SCA attacks.

### A. Experimental Setup

We employ the routing algorithm and software detailed in Section III-A to implement shields with parallel and random parallel topologies, as depicted in Fig. 12, using the top metal layer. In our experiments, we use AES_128 as the experimental circuit, maintaining a clock frequency of 25 MHz, and ILOM operates at 250 MHz. 10K sets of stimuli for each topology are provided, and EM data are simulated by the simulation method in Section III-C. Finally, CEMA is performed on AES_128 with EO-Shield to measure the effectiveness of protection for different topologies.

### B. Evaluation Metric

In addition to Pearson's correlation coefficient and MtD, in this part of the experiment, we choose the signal-to-noise ratio (SNR) as a superior value for evaluating security. In security-related papers, SNR is commonly used to measure the system's level of defense against SCA attacks, which is calculated as follows [32]:

$$SNR = \frac{\rho_{max,corr}}{\rho_{max,incorr}} \tag{4}$$

where $\rho_{max,corr}$ represents the maximum value of the correlation coefficient for the correct hypothetical key across all time points, whereas $\rho_{max,incorr}$ denotes the maximum correlation coefficient for wrong hypothetical keys, representing noise. An average SNR above 1 indicates the presence of side-channel leakage. Conversely, when the SNR falls below 1, the system is considered to exhibit high security against SCA attacks in real-world scenarios where noise is considered.

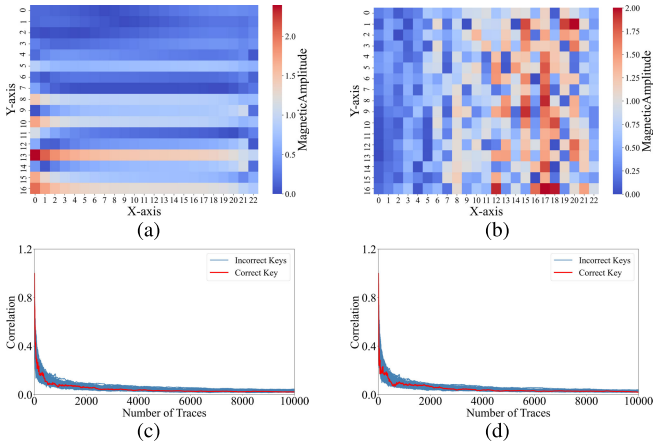



Fig. 13. EM maps and CEMA results of AES_128 with different shield topologies. (a) EM map of AES_128 with a parallel shield. (b) EM map of AES_128 with a random parallel shield. (c) CEMA results of AES_128 with a parallel shield. (d) CEMA results of AES_128 with a random parallel shield.

### C. Experimental Results

Fig. 13 (a) and (b) demonstrate the EM variations brought about by different shield topologies for AES_128 at a specific time point. The distinct routing styles of each topology lead to unique EM distributions, yet both effectively transfer EM hotspots of the AES_128 circuit without protection schemes. This underscores EO-Shield's robust protection ability, which greatly reduces the EM leakage. Additionally, the effectiveness of EO-Shield in thwarting SCA attacks is further corroborated by the correlation analysis results, presented as MtD plots in Fig. 13 (c) and (d).

Next, we examine the SNR results for different shield topologies under 10K sets of stimuli, as depicted in Fig. 14. The analysis reveals that, under the stimuli provided by ILOM, different shields afford comparable levels of protection, with the Hamiltonian structure exhibiting a slight advantage. For practical applications aimed at countering both invasive and non-invasive attacks, the Hamiltonian topology, distinguished by its higher entropy value, is recommended as the primary option.

## VI. Effect of EO-Shield With Different Frequencies

To measure the scalability of the proposed EO-Shield scheme on frequency, we simulate and test the protection effect at three other clock frequencies (200 MHz, 166 MHz 125 MHz). For our benchmark, we still choose the AES_128 circuit, maintaining its clock frequency at 25 MHz, and implement an active shield of Hamiltonian topology to cover the top layer.

TABLE III
COMPARISON OF DESIGNS' OVERHEAD WITHOUT AND WITH EO-SHIELD

| MetricsCircuits | AES_128 (25 MHz) | AES_128 with EO-Shield (250 MHz/200 MHz/166 MHz) | AES_ISEs (25 MHz) | AES_ISEs with EO-Shield (250 MHz/200 MHz/166 MHz) |
|---|---|---|---|---|
| Area | 288195 | 293227 | 376412 | 381444 |
| Percentage increase of area | 1.75% | | 1.34% | |
| Power | 1.51e-2 | 1.65e-2/1.618e-2/1.6e-2 | 2.78e-2 | 2.923e-2/2.888e-2/2.87e-2 |
| Percentage increase of power | 9.47%/7.15%/5.96% | | 5.14%/3.88%/3.24% | |

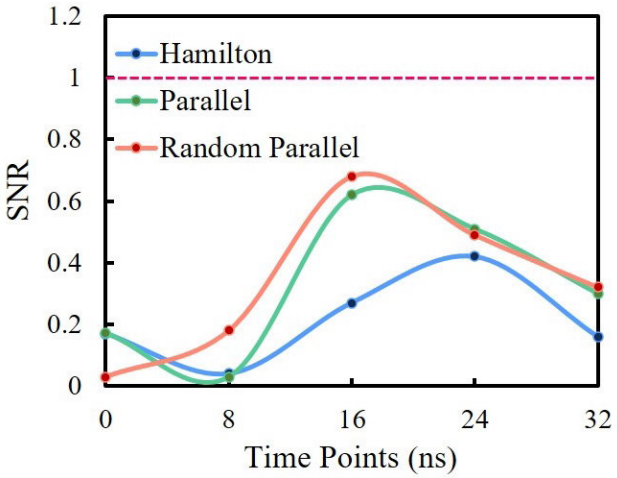



Fig. 14. SNR variation of different shield topologies in the leakage interval.

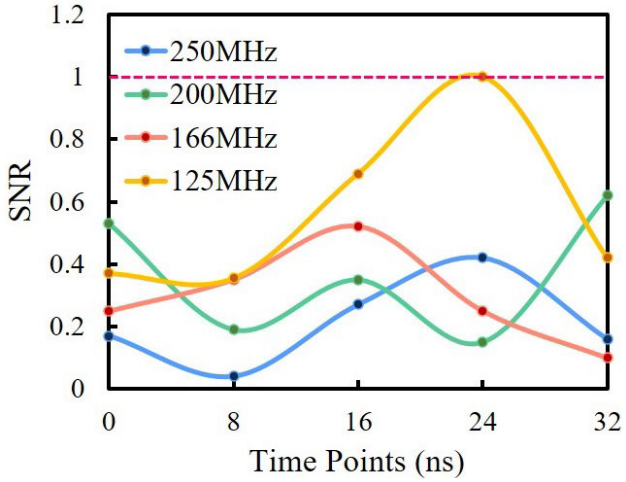



Fig. 15. SNR variation in the leakage interval.

### A. Experimental Results

Fig. 15 shows the SNR ratio traces under different clock frequencies within the leakage interval. The results are also calculated under 10K sets of stimuli. For AES_128 with the clock frequency of 25 MHz, the SNR will appear to reach 1 when the frequency of the EO-Shield scheme is 125 MHz. When the frequency of the EO-Shield scheme is higher than 166 MHz, the SNR of the EM traces detected by the attacker can be kept under 0.6, which greatly improves the level of protection against SCA attacks. Therefore, to obtain the desired side-channel protection, the frequency of the EO-Shield scheme needs to be at least 7 times higher than the frequency of the protected circuit. In this case, even if the attacker analyzes the clock frequency of the protected circuit and finds the location for the attack, he still cannot successfully recover the correct key.

## VII. OVERHEAD EVALUATION

TABLE III compares the overheads of the designs without and with EO-Shield in terms of area and power consumption. We provide the results for AES_128 and AES_ISEs in the table, as these two designs implement the complete encryption process. The clock frequency of AES_128 and AES_ISEs is fixed at 25 MHz, and we measure the overhead of EO-Shield by adjusting the frequency of EO-Shield (250 MHz/200 MHz/166 MHz). Where the area is estimated based on the total cell area generated by the Design Compiler divided by the area of the NANDX2 gate under 180 nm technology node. The power consumption results are calculated by PTPX. It can be seen that our proposed EO-Shield scheme can effectively resist SCA attacks with low overheads.

In addition, we have verified that the active shield will not affect the circuits underneath in terms of functionality [33]. The Process Antenna Effect (PAE) caused by long wire mesh can be eliminated by using jumpers and adding normally closed transmission gates (NC) or diode cells. The time perturbation of the protected circuit due to effects such as parasitic resistance and parasitic capacitance caused by the information leakage obfuscation module is around 0.1 ns, which can be neglected.

## VIII. DISCUSSION AND FUTURE WORK

In the paper, we demonstrate the effectiveness of EO-Shield using three circuits. However, in practical application senoras, EO-Shield still faces potential limitations and requires continuous optimization. As the complexity and size of the circuit increase, more sophisticated shield designs are required to ensure complete coverage and effectively obfuscate EM emanations. Taking into account the production cost and trade-off between resistance to invasive attacks and non-invasive attacks, the active shield does not need to occupy the entire top metal layer. We plan to optimize the shield generation algorithm and design active shields that cover specific modules or appropriately fill blank areas of the layout to provide multi-dimensional protection for the chip.

We also plan to explore the adaptability of EO-Shield to a wider range of circuit types, such as circuits with different operating characteristics and higher complexity. To do this, ILOM can adopt an adaptive noise generation mode that dynamically adjusts based on the behavior and timing characteristics of different circuits. This ensures that the generated confusing signals can effectively resist side-channel attacks. In addition, although experimental results show that EO-Shield has relatively low overhead in terms of power and area, there are still sufficient trade-offs in highly resource-constrained environments.

Finally, in future work, we will consider manufacturing and testing actual chips containing EO-Shield and conducting a more comprehensive security assessment of EO-Shield, such as using template analysis, machine learning analysis attacks, etc., to further enhance the robustness, versatility, and practicality of EO-Shield.

## IX. Conclusion

In this paper, a multi-functional protection scheme called EO-Shield is proposed for the first time to combat both invasive and non-invasive attacks. The core idea is to combine an active shield with an ILOM to mitigate non-intrusive attacks by feeding current stimulus to the active shield in a noise-injection method while against invasive attacks.

When performing a FIB attack on the circuit, the complex active shield can obfuscate the attacker's vision, and detect short-circuit and breakage attacks in real-time. When performing an SCA on the circuit, the current stimulus on the active shield can generate EM noise that hides the EM information of the protected circuit. In this case, the correlation between EM emanations and processing data is also reduced to achieve an SNR lower than 1. Through simulation experiments on 3 cryptographic circuits, the security of the proposed EO-Shield scheme is finally proved through simulation experiments.

## References


[1] E. Ronen, A. Shamir, A. Weingarten, and C. O'Flynn, "IoT Goes nuclear: Creating a ZigBee chain reaction," in *Proc. IEEE Symp. Secur. Privacy (SP)*, New York, NY, USA, May 2017, pp. 195–212.

[2] M. T. Rahman et al., "Physical inspection & attacks: New frontier in hardware security," in *Proc. IEEE 3rd Int. Verification Secur. Workshop (IVSW)*, New York, NY, USA, Jul. 2018, pp. 93–102.

[3] H. Handschuh, P. Paillier, and J. Stern, "Probing attacks on tamper-resistant devices," in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst.* Berlin, Germany: Springer, 1999, pp. 303–315.

[4] R. Spreitzer, V. Moonsamy, T. Korak, and S. Mangard, "Systematic classification of side-channel attacks: A case study for mobile devices," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 465–488, 1st Quart., 2017.

[5] J. He, X. Guo, H. Ma, Y. Liu, Y. Zhao, and Y. Jin, "Runtime trust evaluation and hardware Trojan detection using on-chip EM sensors," in *Proc. 57th ACM/IEEE Design Autom. Conf. (DAC)*, New York, NY, USA, Jul. 2020, pp. 1–6.

[6] M. Weiner, W. Wieser, E. Lupon, G. Sigl, and S. Manich, "A calibratable detector for invasive attacks," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 27, no. 5, pp. 1067–1079, May 2019.

[7] Y. Ishai, A. Sahai, and D. Wagner, "Private circuits: Securing hardware against probing attacks," in *Proc. Annu. Int. Cryptol. Conf.* Berlin, Germany: Springer, 2003, pp. 463–481.

[8] J.-M. Cioranesco et al., "Cryptographically secure shields," in *Proc. IEEE Int. Symp. Hardw.-Oriented Secur. Trust (HOST)*, New York, NY, USA, May 2014, pp. 25–31.

[9] H. Wang, Q. Shi, A. Nahiyan, D. Forte, and M. M. Tehranipoor, "A physical design flow against front-side probing attacks by internal shielding," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 39, no. 10, pp. 2152–2165, Oct. 2020.

[10] T. Miki et al., "Si-backside protection circuits against physical security attacks on flip-chip devices," *IEEE J. Solid-State Circuits*, vol. 55, no. 10, pp. 2747–2755, Oct. 2020.

[11] K. Wang, Y. Gu, T. Zhou, and H. Chen, "Multi-pair active shielding for security IC protection," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 38, no. 12, pp. 2321–2329, Dec. 2019.

[12] P. Laackmann and H. Taddiken, "Apparatus for protecting an integrated circuit formed in a substrate and method for protecting the circuit against reverse engineering," U.S. Patent 6 798 234, Sep. 28, 2004.

[13] G. Xuelian, Z. Dongyan, H. Yi, G. Jie, F. Wennan, and Z. Ran, "An active shielding layout design based on smart chip," in *Proc. IEEE 5th Adv. Inf. Technol., Electron. Autom. Control Conf. (IAEAC)*, vol. 5, Mar. 2021, pp. 1873–1877.

[14] D. Das, S. Ghosh, A. Raychowdhury, and S. Sen, "EM/power side-channel attack: White-box modeling and signature attenuation countermeasures," *IEEE Design Test.*, vol. 38, no. 3, pp. 67–75, Jun. 2021.

[15] D. D. Hwang et al., "AES-based security coprocessor IC in 0.18-$\mu m$ CMOS with resistance to differential power analysis side-channel attacks," *IEEE J. Solid-State Circuits*, vol. 41, no. 4, pp. 781–792, Apr. 2006.

[16] T. Popp and S. Mangard, "Masked dual-rail pre-charge logic: DPA-resistance without routing constraints," in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst.* Berlin, Heidelberg: Springer, 2005, pp. 172–186.

[17] S. Sen and A. Raychowdhury, "Electromagnetic and machine learning side-channel attacks and low-overhead generic countermeasures," in *Proc. CHES*. Accessed: Mar. 19, 2021, pp. 1–19.

[18] X. T. Ngo et al., "Cryptographically secure shield for security IPs protection," *IEEE Trans. Comput.*, vol. 66, no. 2, pp. 354–360, Feb. 2017.

[19] E. Katz, M. Avital, and I. Levi, "Refined analytical EM model of IC-internal shielding for hardware-security and intra-device simulative framework," *IEEE Access*, vol. 12, pp. 22205–22218, 2024.

[20] R. Xin, Y. Yuan, J. He, S. Zhen, and Y. Zhao, "Random active shield generation based on modified artificial fish-swarm algorithm," *Comput. Secur.*, vol. 88, pp. 101552.1–101552.12, Jan. 2020.

[21] 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.

[22] Y. Gao, H. Ma, J. Kong, J. He, Y. Zhao, and Y. Jin, "EMSim+: Accelerating electromagnetic security evaluation with generative adversarial network," in *Proc. IEEE/ACM Int. Conf. Comput. Aided Design (ICCAD)*, Oct. 2023, pp. 1–8.

[23] H. Wu et al., "Focused helium ion beam deposited low resistivity cobalt metal lines with 10 nm resolution: Implications for advanced circuit editing," *J. Mater. Sci. Mater. Electron.*, vol. 25, no. 2, pp. 587–595, 2014.

[24] S. Takarabt et al., "Post-layout security evaluation methodology against probing attacks," in *Proc. Int. Conf. Ind. Netw. Intell. Syst.* Berlin, Germany: Springer, 2021, pp. 465–482.

[25] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proc. 19th Annu. Int. Cryptol. Conf. Adv. Cryptol. (CRYPTO)*, Santa Barbara, CA, USA. Berlin, Heidelberg: Springer, Aug. 1999, pp. 388–397.

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

[27] K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic analysis: Concrete results," in *Proc. 3rd Int. Workshop Cryptograph. Hardw. Embedded Syst. (CHES)*, Paris, France. Berlin, Heidelberg: Springer, May 2001, pp. 251–261.

[28] E. Brier, C. Clavier, and F. Olivier, "Correlation power analysis with a leakage model," in *Proc. 6th Int. Workshop Cryptograph. Hardw. Embedded Syst. (CHES)*, Cambridge, MA, USA. Springer, Aug. 2004, pp. 16–29.

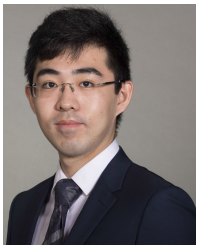
[29] Y. Wang and M. Tang, "A survey of side-channel leakage assessment," *Electronics*, vol. 12, no. 16, p. 3461, Aug. 2023.

[30] S. Briais, J.-M. Cioranesco, J.-L. Danger, S. Guilley, D. Naccache, and T. Porteboeuf, "Random active shield," in *Proc. Workshop Fault Diagnosis Tolerance Cryptogr.*, Sep. 2012, pp. 103–113.

[31] X.-L. Li, "Parameter tuning method of robust PID controller based on artificial fish school algorithm," *Inf. Control*, vol. 33, no. 1, pp. 112–115, Aug. 2004.
[32] I. Levi, A. Fish, and O. Keren, "CPA secured data-dependent delay-assignment methodology," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 25, no. 2, pp. 608–620, Feb. 2017.
[33] Z. Yiqiang et al., "Research on software-defined active shield protection technology," *Acta Electonica Sinica*, vol. 50, no. 6, p. 1381, 2022.


**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.

**Qizhi Zhang** received the B.S. degree in microelectronics from Tianjin University, Tianjin, China, in 2019, where he is currently 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. Prior to the Ph.D. degree, he was a System Software Engineer with Sina Cooperation. His research interests include homomorphic encryption (FHE), post-quantum cryptography (PQC), and cryptography software and hardware co-design and optimization techniques.

**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.

**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.