EO-Shield: A Multi-function Protection Scheme against Side Channel and Focused Ion Beam Attacks

Ya Gao
Tianjin University
Tianjin, China
gaoyaya@tju.edu.cn

Qizhi Zhang
Tianjin University
Tianjin, China
qizhi_zhang@tju.edu.cn

Haocheng Ma
Tianjin University
Tianjin, China
hc_ma@tju.edu.cn

Jiaji He*
Tianjin University
Tianjin, China
dochejj@tju.edu.cn

Yiqiang Zhao
Tianjin University
Tianjin, China
yq_zhao@tju.edu.cn

ABSTRACT

Smart devices, especially Internet-connected devices, typically incorporate security protocols and cryptographic algorithms to ensure the control flow integrity and information security. However, there are various invasive and non-invasive attacks trying to tamper with these devices. Chip-level active shield has been proved to be an effective countermeasure against invasive attacks, but existing active shields cannot be utilized to counter side-channel attacks (SCAs). In this paper, we propose a multi-function protection scheme and an active shield prototype to against invasive and non-invasive attacks simultaneously. The protection scheme has a complex active shield implemented using the top metal layer of the chip and an information leakage obfuscation module underneath. The leakage obfuscation module generates its protection patterns based on the operating conditions of the circuit that needs to be protected, thus reducing the correlation between electromagnetic (EM) emanations and cryptographic data. We implement the protection scheme on one Advanced Encryption Standard (AES) circuit to demonstrate the effectiveness of the method. Experiment results demonstrate that the information leakage obfuscation module decreases SNR below 0.6 and reduces the success rate of SCAs. Compared to existing single-function protection methods against physical attacks, the proposed scheme provides good performance against both invasive and non-invasive attacks.

KEYWORDS

Active shield, electromagnetic side-channel, side-channel security

ACM Reference Format:
Ya Gao, Qizhi Zhang, Haocheng Ma, Jiaji He*, and Yiqiang Zhao. 2023. EO-Shield: A Multi-function Protection Scheme against Side Channel and Focused Ion Beam Attacks. In *28th Asia and South Pacific Design Automation Conference (ASPDAC '23), January 16–19, 2023, Tokyo, Japan.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3566097.3567924

1 INTRODUCTION

Integrated circuits (ICs) have been widely used in various information infrastructures, including electronic payment, Internet of Things (IoT), 5G mobile communications, etc. The embedded devices within those information infrastructures typically incorporate cryptographic algorithms to ensure the confidentiality, authenticity and integrity of security-critical data. However, there are still various attacks trying to tamper the security of ICs. For example, the global AES-CCM key used by Philips Hue, a smart lighting system, to encrypt and authenticate new firmware was successfully recovered by attackers using power SCA [1].

State-of-the-art physical attacks can be generally classified as invasive and non-invasive attacks [2]. Focused ion beam (FIB) attack is the most investigated invasive attack. After the chip is depackaged, the FIB attack can directly alter the metal nets' connections and obtain secret data from the chip, which posts a threat to the chip [3]. Side-channel attack (SCA) tries to extract sensitive information from the chip by collecting and analyzing the physical parameters of the chip. The physical parameters that can be exploited include electromagnetic (EM) emanation, power consumption, timing variations, etc [4]. Compared to other side-channel parameters, EM SCA requires no direct connections to the chips and can obtain local EM information with 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, analog sensors [6], *t*-private circuits [7], internal shields [8] and active shield [9] have been proposed. Among them, the reliability of analog sensors can be affected by advanced technology nodes. The area overhead involved for the transformation of *t*-private circuits is expensive. Internal shields are placed on an internal layer rather than top layer, reducing the area overhead of the circuit, but cannot simultaneously meet the need to counter side-channel attacks. Active shield based solutions are so far the most common countermeasure, which is typically implemented using the top metal layer of the chip, and the shield can proactively detect FIB attacks in real time through monitoring specific dynamic signal sequences within the wire mesh of the shield. To improve the chip's resistance to non-invasive SCAs, various protection methods have been proposed. From the perspective of chip's physical implementations, one important premise is to

ASPDAC '23, January 16–19, 2023, Tokyo, Japan
© 2023 Association for Computing Machinery.
ACM ISBN 978-1-4503-9783-4/23/01…$15.00
https://doi.org/10.1145/3566097.3567924

*: Jiaji He is the corresponding author.

use noise injection (NI) and correlated signature suppression to reduce the SNR [10]. Some representative protection methods include wave dynamic differential logic (WDDL) [11], dual-rail pre-charge (DRP) circuits, sense amplifier-based logic (SABL), etc. However, existing physical protection methods could introduce > 2X overall overheads.

To the best of our knowledge, there exists no multi-purpose protection method that can counter against both invasive and non-invasive attacks simultaneously. It's worth mentioning that existing active shield's monitoring activities can introduce extra noise to the chip's EM emanation [12]. The newly introduced random noise can be properly utilized to lower the EM side-channel SNR and increase the complexity of EM SCAs. In this paper, we propose and implement the *EO-Shield*, Electromagnetic Obfuscation Shield, which is a multi-function protection scheme against both side-channel and FIB attacks. Based on our previously designed active shields [13], we further exploit the noise introduced by the monitoring activities of the active shields to resist EM SCAs. The signals fed into the shield's wire mesh are carefully generated based on the chip's behaviors to obfuscate the chip's EM emanation, and the signal generation module is integrated underneath the active shield. After the chip's and the active shield's emanations are superposed in space, the chip's original EM emanation will be hidden in the overall superposed EM emanation. More specifically, our work makes the following contributions:

- A multi-function protection scheme is proposed to counter against both invasive and non-invasive attacks. Here, we implemented an active shield by using the top metal layer, which can monitor FIB attacks and actively obfuscate EM emanations.
- We developed an information leakage obfuscation module to provide inputs to the active shield. These inputs are generated based on the behavior of the underlying circuit and they are motivated to the active shield to obfuscate the EM side-channel information of the circuit.
- The effectiveness of the proposed multi-function protection scheme is successfully validated through simulation. One AES circuit is developed with EO-Shield scheme and the EM SCAs are performed on the circuit to demonstrate the results.

The remainder of this paper is organized as follows. Section 2 provides the preliminary. The EO-Shield scheme is introduced in Section 3. Section 4 provides the experimental results. The conclusion and discussion are summarized in Section 5.

2 PRELIMINARIES

2.1 Invasive Attacks

Invasive attack is an important method of cracking chips, typically using a series of FIB devices to obtain critical information about the chip via reverse engineering, micro-probing, and other destructive methods. The FIB is a powerful circuit editing tool that can mill and deposit material with high precision on silicon dies, making it simple to cut, connect, and alter the chip's metal alignment [14]. A typical invasive attack is carried out using a FIB workstation and consists of the following four steps [15]:

Reverse engineering: After decapsulating the chip, the attacker extracts the layout and netlist and identifies attack areas.

Locating the target wire: Locate the position of the target line and determine whether the cutting of the metal wire will affect the extraction of the target wire.

Probing pad creating: Create a conductive path for probing, then the key signal is extracted and a metal cross pad is made by FIB equipment.

Extracting target information: Finally the target signal is probed using a probe table staked to the metal pad.

The most important of the four steps is reverse engineering [16], which needs to reconstruct each layer of the chip using microscopic imaging. Therefore, using the top metal layer of the chip to build an active shield can resist invasive attacks.

2.2 Correlation Electromagnetic Attack (CEMA)

CEMA is a common side-channel attack method that uses Pearson's correlation as a statistical method to recover sensitive information by mapping the collected EM traces to sensitive intermediate values. In our threat model, we assume a passive attacker who does not know the sensitive information in the victim chip, but has physical access to the chip and obtain the EM emanations. Fig. 1 shows how CEMA works, with the steps listed below.

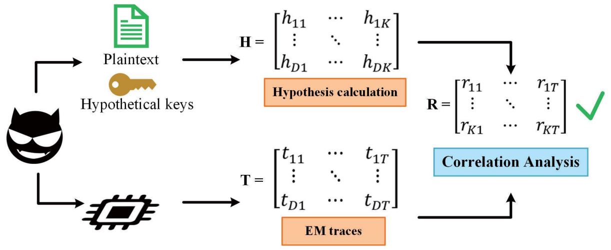

Plaintext
Hypothetical keys
H = [h11 ⋯ h1K; ⋮ ⋱ ⋮; hD1 ⋯ hDK]
Hypothesis calculation
T = [t11 ⋯ t1T; ⋮ ⋱ ⋮; tD1 ⋯ tDT]
EM traces
R = [r11 ⋯ r1T; ⋮ ⋱ ⋮; rK1 ⋯ rKT]
✓
Correlation Analysis

Figure 1: Traditional CEMA

Select the middle value: For the encryption algorithm, the chosen middle value should satisfy the function $f(d,k)$, where d is usually the plaintext and k is part of the key.

Collect the EM traces: Collect the EM traces generated during D times encryption to obtain the EM information leakage matrix T.

Calculate the hypothetical EM information leakage matrix: The Hamming distance or Hamming weight model is used to generate a hypothetical EM information leakage matrix H based on the guessed key values and the known plaintext.

Correlation Analysis: The correlation between the matrices T and H is calculated using the Eq. (1) to yield the correlation matrix R, where the guessed key with the highest correlation is the true key.

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

2.3 Signal-to-Noise-Ratio (SNR)

In security-related scenarios, SNR [17] is commonly used to measure the system's level of resisting SCAs and is calculated as Eq. (2):

$$SNR = \frac{\rho_{corr}}{\rho_{max,incorr}} \tag{2}$$

where ρ_{corr} is the correlation coefficient of the correct key and $\rho_{max,incorr}$ is the maximum correlation coefficient of the incorrect key. When SNR drops below 1, the system is considered to be able to resist SCAs in a real-world scenario where noise is considered.

3 MULTI-FUNCTION PROTECTION SYSTEM DESIGN

The proposed EO-shield protection scheme framework is depicted in Fig. 2, which contains an active shield and an information leakage obfuscation module. In our framework, the active shield is generated and designed to cover the protected area of the chip, while the information leakage obfuscation module is designed to monitor invasive attacks and to generate signals that can induce extra EM emanation in the wire mesh. More specifically, when an invasive attack happens, such as the active shield is being cut off or shorted, the module underneath will give out an alert signal. Meanwhile, the signals motivated into the wire mesh can obfuscate the EM side-channel information to further improve the resistance to SCAs.

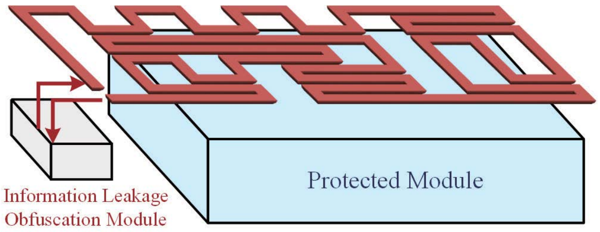


Figure 2: The architectural of EO-Shield

3.1 Random Active Shield Design and Implementation

The active shield is usually implemented utilizing the top metal layer of the chip and is required to have a high level of complexity. At present, the commonly used active shields are serpentine, parallel, Hilbert curve, Peano curve and random Hamiltonian topologies. Among them, the random Hamiltonian topology has the highest randomness and hard to be attacked. In this paper, we focus on the EO-shield protection system, so we will use the available algorithm to generate active shield. Based on our previous work, we use the shield generation software to produce active shields with random Hamiltonian topology based on an Artificial Fish-Swarm Random Hamiltonian algorithm (AFSRHA) [18].

Fig. 3 shows the execution process of AFSRHA. We define the length and width of the shield area as L and W, respectively. The wire width and wire space of wire mesh are represented by *wire_width* and *wire_space*. L and W are normalized into grid points by *wire_width* and *wire_space*, and a square formed by four adjacent grid points is defined as a fish. A fish is randomly selected and merged with an adjacent fish to generate a loop C. Next, a fish adjacent to loop C is randomly selected and merged into loop C. Repeat this process until all the fish are included in loop C and the active shield generation is completed.

The AFSRHA algorithm requires that L and W satisfy:

$$L, W \geq 8 \times (wire\_width + wire\_space) \tag{3}$$

When L or W does not satisfy Eq. (3), for example, the shield area is the gap between the dense power strips on the top layer. We call this case a narrow, elongated shield area and propose the 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.

3.2 Information Leakage Obfuscation Module Design and Noise Signal Generation

The purpose of the information leakage obfuscation module is to generate noise signals. The EM emanations generated by these signals on the active shield will obfuscate the EM emanations of the underlying protected circuits in the form of NI. The architecture of the module is shown in Fig.5, which mainly consists of three parts: the linear feedback shift register (LFSR), the RO oscillation circuit, and signal comparison module. LFSR is the most common method of generating pseudo-random numbers, which is based on the principle of Primitive Polynomial, consisting of several D flip-flops and XOR gates. The random signals generated by the LFSR will be motivated into the active shield. In practice, it is possible to choose the appropriate Primitive Polynomial flexibly according to the stochasticity requirement. For example, for a 15-bit LFSR, Eq. (4) can be used to achieve the maximum number of output states.

$$x^{15} + x + 1 \tag{4}$$

The EM noise generated by the RO oscillation circuit is used to mask the EM emanations generated during the combinational logic operation of the protected circuit. Since the number of inverters is proportional to the time delay, we design four RO oscillation circuits with the number of inverters of 3, 5, 7 and 9 respectively, which have gradually increasing time delays. The signal comparison module compares the random signal that fed into the active shield with the signal output from the active shield to achieve real-time monitoring of invasive attacks. Once the comparison fails, an alarm signal will be triggered.

Note that, the clock frequency of the protected circuit is generated by dividing the clock frequency of the information leakage obfuscation module, making it more difficult for an attacker to guess. Suppose the clock period $t_{proteced}$ of the protected circuit contains n clock periods $t_{obfuscation}$ of the information leakage obfuscation module. According to the pseudo-random number generation law, the probability that the generated pseudo-random number signal remains constant during the time of t_{pro} is $1/2^{n-1}$. Therefore, the clock frequency of the information leakage obfuscation module must be high to ensure that there are enough changing pseudo-random number signals for signal comparison.

Here we name the high-frequency clock of the information leakage obfuscation module as *clk*, and name the divided low-frequency clock, which is the clock of the protected circuit, as *clk_chip*. Usually the protected circuit will start executing combinational logic operations after the clock edge arrives, so the multiplexer in Fig. 5 outputs a random signal or RO oscillation signal by detecting the clock edge of the protected circuit .

Fig. 6 illustrates the attacker's CEMA process on an EO-shield protected chip. Since the active shield is closer to the EM probe

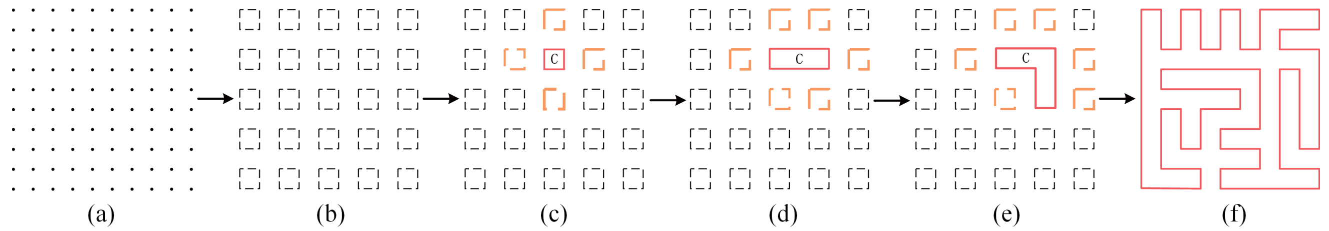


Figure 3: The execution process of AFSRHA algorithm.

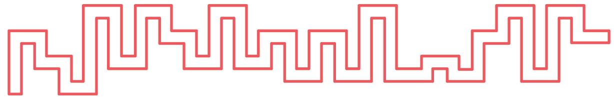


Figure 4: Random Parallel Shield

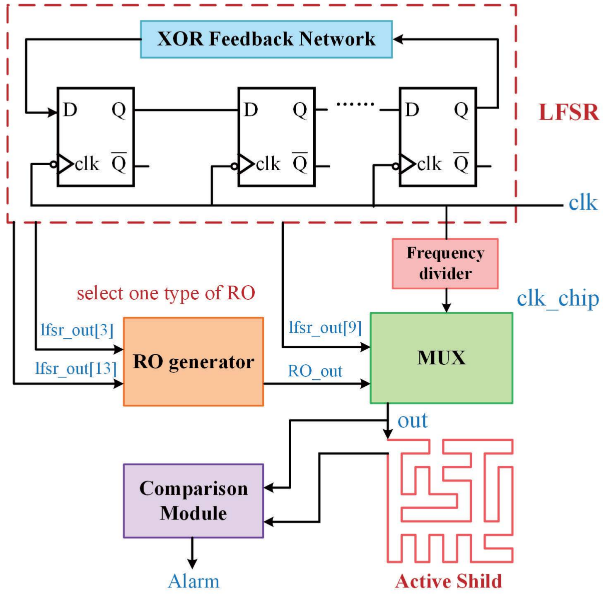


Figure 5: Information obfuscation circuit

and is fed with the signal generated by the information leakage obfuscation module, the actual EM information leakage matrix T measured by the attacker also contains the noise magnetic field (i.e. $n_{1,1}, n_{1,2}......n_{D,T}$) generated by the active shield. In this way, the noise-injected EM information leakage matrix cannot be exploited to recover the sensitive information when correlation analysis is performed with the hypothetical EM information leakage matrix.

4 EXPERIMENT AND RESULT

In this section, the AES implementation we choose is designed in the light of NIST standard, denoted as AES_NIST, which includes 128-bit plaintext and key [19]. In our previous work [20], we have generated several different active shields. Experimental results have verified that they can successfully detect invasive attacks and trigger the alarm signal. Thus, in this paper we will mainly demonstrate the effectiveness of the robustness of the scheme against CEMA.

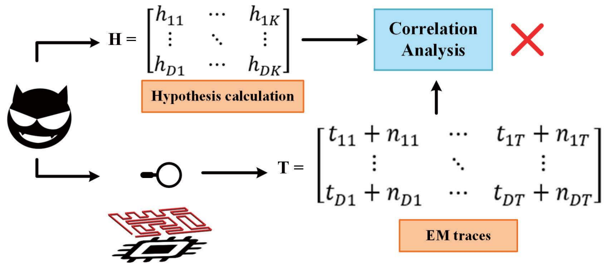

$H = \begin{bmatrix} h_{11} & \cdots & h_{1K} \\ \vdots & \ddots & \vdots \\ h_{D1} & \cdots & h_{DK} \end{bmatrix}$
Hypothesis calculation
Correlation Analysis
$T = \begin{bmatrix} t_{11}+n_{11} & \cdots & t_{1T}+n_{1T} \\ \vdots & \ddots & \vdots \\ t_{D1}+n_{D1} & \cdots & t_{DT}+n_{DT} \end{bmatrix}$
EM traces

Figure 6: CEMA with an EO-Shield

The simulation setting is initially provided. We then develop a simulation model of an AES_NIST chip with an active shield and an information leakage obfuscation module to verify the effectiveness of the proposed EO-shield scheme.

4.1 Experiment Setup

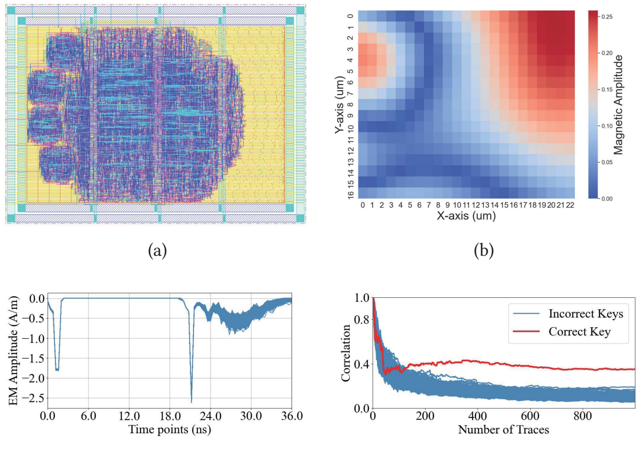
We use the EMSim (Electromagnetic emanation Simulation at early design phrase) tool [21] to model the EM simulation of an unprotected AES circuit and an AES circuit protected with an EO-shield scheme, respectively. Then, CEMA is performed for both circuits. The entire design is realized using 180 nm technology with a nominal voltage V_{dd} of 1.8 V.

Specifically, at the layout level, the Star RCXT tool is first used to extract the parasitic resistors and parasitic capacitors at the logic cell level and generate a file in DSPF format. Then we perform parasitic network simplification. Next, the power consumption of each logic cell at the layout level netlist is simulated using PrimeTime tool and current stimuli are generated. The DSPF file and the current stimuli are combined into a Spice netlist file, which is input to the HSpice tool to calculate the transient current distribution in the parasitic network. With the help of layout information, the current distribution is corresponded to the plate coordinates and the EM distribution on the chip surface is calculated using the Biot-Savart Law. Finally, we perform the CEMA described in Section 2.2. Pearson correlation coefficient, minimum trace of disclosure key (MtD) and SNR are used as security metrics, which are widely used in the field of hardware security.

4.2 CEMA on Unprotected AES Circuit

In this subsection, CEMA is performed on the unprotected AES circuit. Fig. 7(a) shows the physical layout of the 128-bit AES chip generated using 180 nm CMOS technology, with a die size of the total chip occupies 1140μm×840μm, implemented with 5 metal layers, and the clock frequency is 25 MHz.

For AES circuits, the byte substitution operation of the S-BOX is a common location for side-channel attacks, so the EM traces of the AES circuit during the first round of byte substitution operation time (one clock cycle) is simulated using the EMSim tool and a leakage model is constructed. The EMsim tool divides the chip surface into 23×17 sub-regions for EM calculations. For an unprotected AES circuit, given 1000 random plaintext inputs, the EM maps and EM traces simulated by the EMSim tool are shown in Fig. 7(b) and Fig. 7(c) respectively. The EM map clearly shows that the upper right corner of the chip has a large EM leakage, so the focus is on this area for CEMA.



(a) (b)

(c) (d)

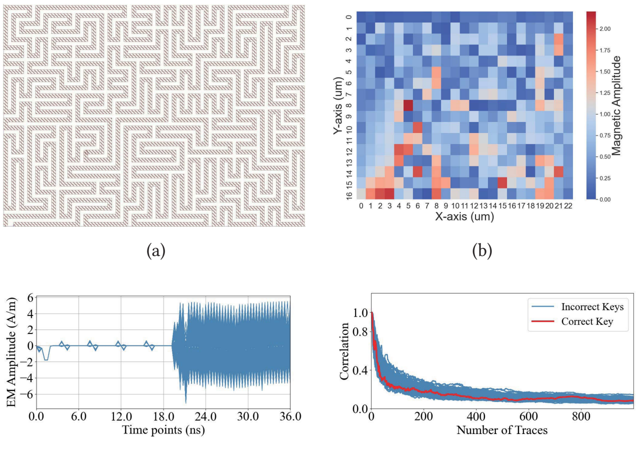
Figure 7: CEMA results on unprotected AES circuit. (a) Chip layout of AES. (b) EM map of the chip surface (23×17). (c) EM traces of the SubByte operation in the first S-Box. (d) MtD results.

Security Evaluation. Fig. 7(d) illustrates the CEMA results of the unprotected AES circuit, with the x-axis representing the number of traces needed for a successful attack and the y-axis representing the correlation coefficient. The highest correlation coefficient for the correct guessed key can reaches above 0.35 and can be distinguished from other guessed key traces within 124 traces, MTD = 124.

4.3 CEMA on Protected AES Circuit

The active shield covering the AES circuit is generated using the top metal layer of 180 nm CMOS technology, as shown in Fig. 8(a). During the S-BOX operation, the information leakage obfuscation module starts operating at 250 MHZ and generates the current stimulus delivered to the active shield. For the same 1000 random plaintext inputs, the EM simulation was performed using the EMSim tool and CEMA was performed.

Security Evaluation. When the AES circuit is protected under the EO-shield scheme, the leakage hotspots in the EM map (Fig. 8(b)) are hidden and transferred at the same time. Besides, the EM emanations generated by the circuit encryption process is hidden in the noise generated by the information leakage obfuscation module (Fig. 8(c)) and the correct key cannot be recovered (Fig. 8(d)).



(a) (b)

(c) (d)

Figure 8: CEMA results on protected AES circuit. (a) The active shield. (b) EM map of the chip surface (23×17). (c) EM traces of the SubByte operation in the first S-Box. (d) MtD results.

4.4 Scalability of EO-shield Scheme on Frequency

To measure the scalability of the proposed EO-shield scheme on frequency, we tested the protection effect at three other clock frequencies (200Mhz, 166Mhz, 125Mhz). Here we use SNR as a superior value for evaluating security, and Fig. 9 shows the SNR traces at different clock frequencies within the leakage interval.

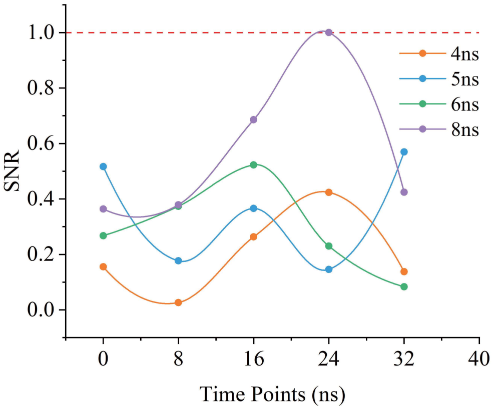


Figure 9: SNR variation in the leakage interval.

Security Evaluation. For the AES circuit 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 SCAs. Therefore, in order to obtain the desired side-channel protection, the frequency of the EO-shield scheme needs to be at least 7 times higher than

Table 1: Comparison of the overhead of unprotected AES circuits and AES circuits with EO-shield.

Circuits Metrics	Unprotected AES (25MHZ)	AES with EO-shield (250MHZ/200MHZ/166MHZ)	Increase Percentage
Area (μm^2)	288195	293227	1.75%
Power (w)	$1.51e-2$	$1.65e-2/1.618e-2/1.6e-2$	9.74%/7.15%/5.96%

the frequency of the protected circuit. In this case, even if the attacker analyzes the clock frequency of the AES circuit and finds the location for attack, he still cannot successfully recover the correct key.

4.5 Overhead Evaluation

Table 1 compares the overheads in terms of area and power consumption of the unprotected AES circuit and the AES circuit with EO-shield. Where, the area is estimated based on the total cell area generated by Design Complier divided by the area of NANDX2 under 180nm process. The power consumption results are calculated by PrimeTime PX. It can be seen that our proposed EO-shield scheme can effectively resist SCAs with low overheads.

In addition, we have verified that the active shield will not effect the circuits underneath in terms of functionality. The Process Antenna Effect (PAE) caused by long wire mesh can be eliminated by using jumpers, 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 0.1ns, which can be neglected.

5 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 information leakage obfuscation module 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 a 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 a SNR lower than 1. Through simulation experiments, the security of the proposed EO-shield scheme is finally proved through simulation experiments. In the future, we will consider measuring physical EM signals, which will strengthen the proposed method.

In practice, considering production costs and the trade-off between resistance to invasive attacks and SCAs, the active shield does not need to occupy the entire top metal layer. It only needs to ensure that it can cover the modules with a large amount of information leakage, as well as properly fill the blank areas of the layout, to provide multi-dimensional protection for the chip.

ACKNOWLEDGMENTS

This research is supported by the Science and Technology Project of the Headquarters of State Grid Corporation of China, Research on Key Techniques in Reliability of Low Power Sensor Chip for IOTIPS (No.5700-202041397A-0-0-00).

REFERENCES

[1] E. Ronen, A. Shamir, A. O. Weingarten, et al. Iot goes nuclear: Creating a zigbee chain reaction. In *2017 IEEE Symposium on Security and Privacy (SP)*, pages 195–212, New York, NY, USA, 2017. IEEE.

[2] M. T. Rahman, Q. Shi, S. Tajik, et al. Physical inspection attacks: new frontier in hardware security. In *2018 IEEE 3rd International Verification and Security Workshop (IVSW)*, pages 93–102, New York, NY, USA, 2018. IEEE.

[3] H. Handschuh, P. Paillier, and J. Stern. Probing attacks on tamper-resistant devices. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 303–315, Berlin, Germany, 1999. Springer.

[4] R. Spreitzer, V. Moonsamy, T. Korak, et al. Systematic classification of side-channel attacks: A case study for mobile devices. *IEEE Communications Surveys & Tutorials*, 20(1):465–488, 2017.

[5] J. He, X. Guo, H. Ma, et al. Runtime trust evaluation and hardware trojan detection using on-chip em sensors. In *2020 57th ACM/IEEE Design Automation Conference (DAC)*, pages 1–6, New York, NY, USA, 2020. IEEE.

[6] M. Weiner, W. Wieser, E. Lupon, et al. A calibratable detector for invasive attacks. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 27(5):1067–1079, January 2019.

[7] Y. Ishai, A. Sahai, and D. Wagner. Private circuits: Securing hardware against probing attacks. In *Annual International Cryptology Conference*, pages 463–481, Berlin, Germany, 2003. Springer.

[8] W. Huanyu, S. Qihang, N. Adib, et al. A physical design flow against front-side probing attacks by internal shielding. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 39(10):2152–2165, 2019.

[9] J. M. Cioranesco, J. L. Danger, T. Graba, et al. Cryptographically secure shields. In *IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, pages 25–31, New York, NY, USA, 2014. IEEE.

[10] D. Das, S. Ghosh, A. Raychowdhury, et al. Em/power side-channel attack: White-box modeling and signature attenuation countermeasures. *IEEE Design Test*, 38(3):67–75, 2021.

[11] D. D. Hwang, K. Tiri, A. Hodjat, et al. Aes-based security coprocessor ic in 0.18-*muhboxm*cmos with resistance to differential power analysis side-channel attacks. *IEEE Journal of Solid-State Circuits*, 41(4):781–792, 2006.

[12] T. N. Xuan, J. L. Danger, S. Guilley, et al. Cryptographically secure shield for security ips protection. *IEEE Transactions on Computers*, 66(2):354–360, 2016.

[13] R. Xin, Y. Yuan, J. He, et al. Random active shield generation based on modified artificial fish-swarm algorithm. *Computers & Security*, 88:101552.1–101552.12, 2020.

[14] H. Wu, L. A. Stern, D. Xia, et al. Focused helium ion beam deposited low resistivity cobalt metal lines with 10nm resolution: implications for advanced circuit editing. *Journal of Materials Science Materials in Electronics*, 25(2):587–595, 2014.

[15] S. Takarabt, S. Guilley, Y. Souissi, et al. Post-layout security evaluation methodology against probing attacks. In *International Conference on Industrial Networks and Intelligent Systems*, pages 465–482, Berlin, Germany, 2021. Springer.

[16] Shahed, E., Quadir, Junlin, et al. A survey on chip to system reverse engineering. *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, 13(1), 2016.

[17] I. Levi, A. Fish, and O. Keren. Cpa secured data-dependent delay-assignment methodology. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 25(2):608–620, August 2016.

[18] L. I. Xiao-Lei, S. H. Feng, J. X. Qian, et al. Parameter tuning method of robust pid controller based on artificial fish school algorithm. *Information Control*, 33(1):112–115, August 2004.

[19] AES. https://github.com/secworks/aes, 2014.

[20] Y. Zhao, Y. Gao, H. Ma, et al. Research on software-defined active shield protection technology. *Acta Electronica Sinica*, 50(6):1381–1388, June 2022.

[21] EMSim. https://github.com/jinyier/EMSim, 2021.