Journal of Electronic Testing (2024) 40:723–740
https://doi.org/10.1007/s10836-024-06155-1

RESEARCH

Multi-modal Pre-silicon Evaluation of Hardware Masking Styles

Md Toufiq Hasan Anik[1] · Hasin Ishraq Reefat[1] · Wei Cheng[2,3] · Jean-Luc Danger[2] · Sylvain Guilley[2,3] · Naghmeh Karimi[1]

Received: 4 March 2024 / Accepted: 25 November 2024 / Published online: 16 December 2024

Abstract
Protecting sensitive logic functions in ASICs requires side-channel countermeasures. Many gate-level masking styles have been published, each with pros and cons. Some styles such as RSM, GLUT, and ISW are compact but can feature 1st-order leakage. Some other styles, such as TI, DOM, and HPC are secure at the 1st-order but incur significant overheads in terms of performance. Another requirement is that security shall be ensured even when the device is aged. Pre-silicon security evaluation is now a normatively approved method to characterize the expected resiliency against attacks ahead of time. However, in this regard, there is still a fragmentation in terms of leakage models, Points of Interest (PoI) selection, attack order, and distinguishers. Accordingly, in this paper we focus on such factors as they affect the success of side-channel analysis attacks and assess the resiliency of the state-of-the-art masking styles in various corners. Moreover, we investigate the impact of device aging as another factor and analyze its influence on the success of side-channel attacks targeting the state-of-the-art masking schemes. This pragmatic evaluation enables risk estimation in a complex PPA (Power, Performance, and Area) and security plane while also considering aging impacts into account. For instance, we explore the trade-off between low-cost secure styles attackable at 1st-order vs high-cost protection attackable only at 2nd-order.

Keywords Side-channel attacks · Masking schemes · Circuit aging · Correlation power analysis · Side-channel distinguisher · 2nd-order · PPA

1 Introduction

Protecting cryptographic circuits against Side-Channel Analysis (SCA) is a concern. Indeed, solid protections come at the expense of a serious burden, in terms of design time and gate count. Design time negatively impacts time-to-market, whereas gate count negatively impacts (proportionally) the final product cost. Thereby, masking hardware circuits requires the designer to make difficult trade-offs between security and design time/cost. A fair objective is to attain at least 1st-order security, which can be brought by masking schemes. Furthermore, it is favorable if security is maintained over the device's lifetime, i.e., it is not diminished by device aging.

Profiling attacks (e.g., template attacks) are devastating yet in such attacks, the adversary has full control on one copy of the device (and its key) and builds a model based on the power traces of such profiling chip to attack another copy of the chip (having a different key) [1]. As full control on one copy of the chip is not always feasible, profiling attacks are not always on the table. Thus, non-profiling attacks, e.g., Correlation Power Analysis (CPA) attacks are considered where the cryptographic device can be attacked even without prior "open" (e.g., with chosen or known key) device characterization.

To prevent SCA, several masking schemes have been proposed in literature, e.g. [2–8]. In general, masking countermeasures [9] can be defeated in two ways:

1. by "frontal" attacking the masking scheme, leveraging a state-of-the-art 2nd-order attack, or
2. by exploiting "defects" in the implementation, such as glitches, which would show up unexpectedly and be correlated at the 1st-order with the device secret.

Glitches in hardware implementations of cryptographic algorithms have first been reported by Mangard et al. [10]. Although later been held responsible for 1st-order leak-

Responsible Editor: A. Orailoglu

Md Toufiq Hasan Anik and Hasin Ishraq Reefat contributed equally to this work

Extended author information available on the last page of the article age in otherwise perfectly masked schemes [11], this threat has never been completely characterized. For instance, only few studies aim at exploiting glitches in practice. Note that glitches are spurious and swift in nature – i.e, hard to harvest in an attack. For instance, the work of Liu et al. allows to reduce only by a mere 29% the number of traces to recover the key in an unprotected (i.e., unmasked) implementation [12, Table IV].

Industry is very careful about implementation size. Thus, an implementation that leaks in 1st-order owing to glitches can well be acceptable in terms of security[1]. To restate, it is not because an implementation has a (potential) 1st-order leakage that it must be abandoned [13]. The real question is whether the estimated 1st-order leakage is strong enough, in particular outperforming that of a natural attack (i.e., the 2nd-order).

In practice, multiple factors can affect the success of a SCA attack including the leakage model, correlation distinguisher, selection of Points of Interest (PoIs), the attack order, etc. However, the previous work in this area is mainly fragmented in case that only one (or two) of these essential players are considered in each research; thus, the result is not conclusive. In other words, there is a need to provide a designer (who opts to select a masking scheme) with some security versus PPA criteria where the security has been extensively analyzed from different angles so he can prioritize one masking scheme over another based on the budget and design constraints. As an example of the shortcoming of the previous work, we can point to [14] which mentions that Hamming Distance (HD) leakage model is always more powerful than the Hamming Weight (HW) model but as we shown in the experimental results, this is not always the case and the attack success depends on many different factors simultaneously. To the best of our knowledge, this is the first paper that compares the state-of-the-art masking schemes from different corners. Our contributions include:

- Showing the complexity of security analysis in pre-silicon as the security is affected by many corners (e.g., leakage model, distinguisher, PoI, attack order, etc) yet the state-of-the-art work mainly concentrates on few corners;
- Comparing the state-of-the-art masking schemes in terms of security vs. PPA to enable the designers to select the appropriate countermeasure based on the budget;
- Analyzing the impact of aging on the security of the state-of-the-art masking schemes to investigate if these schemes will provide long-lasting security or otherwise their security diminishes over time.

In sum, the novelty of this paper is not on attacking masking schemes, yet we focus on leakage exploitability by pushing one step further than detecting leakage via TVLA (Test Vector Leakage Assessment) [15] *or modeling leakage* [16]. We consider a multi-modal security versus PPA analysis for the state-of-the-art masking schemes not only to compare them in terms of this criteria but also to show that multiple factors affect the security together.

Target circuits: The state-of-the-art consists in different masking styles, namely:

- logic styles such as GLUT [2], RSM [3] and its RSM-ROM refinement [4], ISW [5], all of which are subject to glitches possibly demasking the sensitive variable transiently;
- glitch-resistant countermeasures (TI [6], DOM [7], HPC [8], etc.) which are 1st-order secure yet very expensive in terms of PPA.

This paper considers both categories of masking styles, *retaining only TI as representative for glitch-resistant protection*. We notice that all those masking schemes are taken 1st-order, meaning that all fail to protect when attacked at 2nd-order. Table 1 compares the targeted masking styles and unprotected LUT regarding thr number of gates (with 2-4 inputs), equivalent gates (#gates normalized by the number of equivalent 2-input NAND gates), random bits, propagation delay, and average energy.

2 Prior Work on Security Evaluation and Masking schemes

Pre-silicon evaluation has received a lot of attention as it allows to derisk the side-channel threat. It has been popularized with Common Criteria (CC) Protection Profile (PP) 0117 [17], which accepts as a boundary a Security Sub-System (3S) within a System on Chip. The PP 0117 has been certified by the German BSI in 2022 [18] acknowledging pre-silicon evaluation as a licit methodology.

Security metrics have been put forward and security-oriented design-time evaluation was pioneered by Huiyun Li et al. [19]. Recently, the ISO/IEC 17825 standard has also been promoting side-channel evaluation by leakage detection techniques. However, being detection-focused, this international standard is not addressing some practicalities, such as the influence of the selection of PoIs, of the model, etc. To fill the gap, in this paper, we incorporate security analysis based on independent 1st- and 2nd-order attacks while considering the impact of leakage model, distinguisher, PoI, and aging.

S-Box Implementations: We target the following Implementations of PRESENT cipher in this paper:

[1] E.g., the security scheme accepts low AVA_VAN level, as in SESIP level 3.

Table 1 Gate-level Spec. of the targeted PRESENT S-Box Implementations

	LUT	GLUT	RSM	RSM-ROM	ISW	TI
Total Gates	14	772	228	1242	57	1325
Total Equ. Gates	29	1183	373.5	987	112.5	2369
Max. Delay (ps)	280	420	350	1700	470	480
Avg. Energy (mJ)	9.29	149.13	47.53	240.59	50.06	874.58
# Random Bits	0	8	4	4	4	12

The worst cases are highlighted

1) LUT: Look-Up Table is the simple data-flow description of the unprotected S-Box.
2) GLUT: GLUT realizes function $\mathbb{F}_2^4 \times \mathbb{F}_2^4 \times \mathbb{F}_2^4 \rightarrow \mathbb{F}_2^4$ that satisfies $Y = GLUT(A, MI, MO)$, such that $Y \oplus MO = S(A \oplus MI)$ [2]. A and Y are masked input and output. MI and MO denote the input and output masks, respectively.
3) RSM: In Rotating S-Box Masking [3] the mask set is a subset of the full mask set (ref. to as "low-entropy" [20]) and the output masks are derived systematically from the input masks [21]. In our implementation $MO = (MI + 1)$ mod 16 where $0 \leq MI, MO \leq 15$ are integer s (like [3]) and selected such that we have:
$RSM(A, MI)$=$GLUT(A, MI, (MI + 1)$ mod 16).
4) RSM-ROM: ROM-based RSM (a stronger version of RSM) is realized using Read-only memories. Here we target logic designs built only from the instantiation of gates in a Boolean library, following the precepts of [4].
5) ISW: To prevent the undermining of masking security by EDA tools, Ishai, Sahai, and Wagner [5, 22] proposed a bottom-up approach. For non-linear gates, they recommend beginning with a netlist that's optimized in terms of AND/OR usage [23, §3] and then systematically replacing the gates with their related gadgets. Here, AND needs 1-bit of uniformly random data (R). For a random sharing (A_0, A_1) of bit A (where $A = A_0 \oplus A_1$), and same for bit B, their AND is:

$$\begin{cases} Y_0 = ((A_1 \wedge B_1) \oplus R) \oplus (A_0 \wedge B_0) \\ Y_1 = ((A_0 \wedge B_1) \oplus R) \oplus (A_1 \wedge B_0) \end{cases}$$

In these equations, the implementation must follow the order specified within the parentheses in the formula, at least in a static context. Yet as gates evaluate in a non-natural order due to races, ISW may exhibit 1st-order leakage [24] (glitches).
6) TI: TI is a stronger countermeasure and relies on multi-party computation and secret sharing [25]. It maintains non-completeness, correctness, and uniformity properties. Like ISW, TI divides each input bit into $n + 1$ shares, yet TI doesn't need gate ordering. In TI, each output share depends on only n shares of each input; preventing disclosure of unmasked values due to races or glitches (non-completeness property). Thus, TI effectively guards against glitches but requires manual netlist creation and is *more costly than the above masking schemes*.

3 Research Background on Attack Parameters

Here we discuss the factors affecting the success of CPA attacks.

3.1 Leakage Models

The leakage model characterizes the leakage behaviors of the target device when it is running. In CPA, a leakage model is utilized to map the key-dependent sensitive values to estimate the hypothetical leakage [26], which then is used for launching attacks. In practice, two representative leakage models are HW and HD, which mimic leakages caused by the elementary behaviors of CMOS gates [10] where $HW(X)$=$\sum_{i=0}^{n-1} X_i$, $HD(X, Y)$=$HW(X \oplus Y)$ for n-bit variables X and Y.

3.2 Attack Order

A d^{th}-order masking is designed against the d^{th}-order attacks, especially correlation analysis, while it can be compromised by $(d$+$1)^{th}$-order attacks [5]. For instance, for the 1st-order masking schemes, e.g., RSM and ISW, the 2nd-order CPA [27] can recover the key even without the glitches. While in the presence of glitches, certain 1st-order leakages shall occur and then being exploited by the 1st-order CPAs. Therefore, we investigate both the 1st-order and 2nd-order CPAs to evaluate the side-channel resistance of the targeted masking schemes.

3.3 Correlation Analysis: Pearson vs. Spearman

In the category of non-profiling attacks, one of the most efficient attacks is the CPA by using Pearson correlation coefficient [28], and was then extended by using Spearman correlation coefficient [29] for capturing certain non-linear leakages. Recall that Pearson correlation is a measure of linear relationship, whereas Spearman correlation can capture non-linear relationship, provided it is monotonic. Also, Spearman is less sensitive to outliers.

Despite the apparent advantage of Spearman over Pearson correlation, we underline that neither of them can detect 2nd-order leakage. Let us consider the 2nd-order leakage depicted

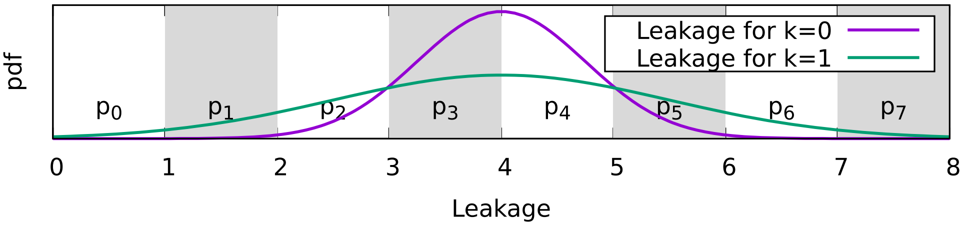

Fig. 1 Example of 2nd-order leakage probability distribution function (pdf) for two values of the key k to recover

in Fig. 1. The octiles of the pdf denote to p_i, for $0 \leq i \leq 7$, where $\sum_i p_i = 1$ and the p_is depend on the key. Owing to leakage symmetry, $p_i = p_{7-i}$.

- The 1st-order Pearson correlation correlates with the average of the distribution, that is 4 for both key values;
- The 1st-order Spearman correlation correlates with the average rank, i.e., $\sum_i i \cdot p_i$, which neither depends on the key. Indeed, the result $\sum_{i=0}^{7} i \cdot p_i = \sum_{i=0}^{3} (i+7-i) \cdot p_i = 7/2$ is a constant.

3.4 Selecting Point of Interest (PoI)

To reduce the attack cost, selecting PoI from the collected power traces has been introduced in literature. However, wrong PoIs can poison the key recovery. SOST (Sum Of Squared pairwise T-differences) [30, §10] and MIA (Mutual Information Analysis) [31] are two main methods used for selecting PoIs in 1st- and 2nd-order attacks, respectively. In this paper, we use these methods and show that they may not be always useful in finding the security flaws in pre-silicon for masked circuits.

3.5 Device Aging

We investigate the resiliency of new and aged masking circuits against CPA. Due to device aging, the delay and power consumption of the gates change over time. Negative Bias Temperature-Instability (NBTI), Positive Bias Temperature Instability (PBTI), and Hot-Carrier Injection (HCI) are the most prominent aging mechanisms [32, 33]. NBTI and PBTI affect PMOS and NMOS transistors, respectively, when they are ON resulting in the increase of the magnitude of the threshold voltage (V_{th}). When the transistor is OFF, the NBTI / PBTI effects partially recover. HCI occurs in NMOS devices when the transistor's gate input switches; shifting its V_{th} and drain current.

4 Evaluation Strategy

Typically, dth-order masking resists against attacks up to dth-order, yet considering their combinational logic, they can be susceptible to inevitable glitches [10] resulting in low-order leakage in some masked circuits [11]. Hence, it is critical to characterize the leakages thoroughly during the pre-silicon security analysis to avoid post-silicon leakage. Accordingly, we performed a thorough security assessment that exploits the glitches of a design via conducting multi-modal 1st- and 2nd-order CPA attacks. The analysis helps the designer to trade-off between low-cost secure styles attackable at 1st-order vs. high-cost protections attackable only at higher orders. The notion behind conducting a multi-modal security evaluation is to systematically appraise the intrinsic security of a device across diverse dimensions. Variations in the leakage model, distinguisher, and device aging introduce potential alterations to the PoIs and the overall vulnerability profile of the device (see Sec. 5). Figure 2 depicts the 2-step performed analysis:

Step 1. Trace collection: To perform pre-silicon security evaluation, we should rely on simulations to acquire power traces. Aging effects are also assessed during Spice simulation for their possible impact on adding or removing glitches. Power traces should be collected for both new and aged devices. In this research the power traces are noise-free as *this is a white-box evaluation for verifying intrinsic security in pre-silicon stage*. We expect post-silicon security analy-

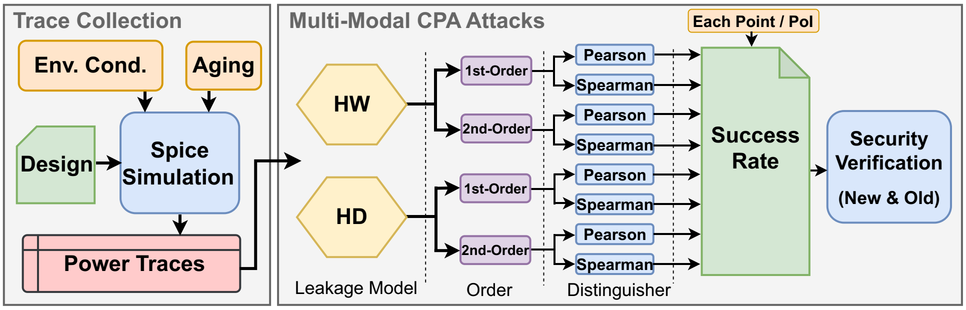

Fig. 2 Deployed framework for pre-silicon security assessment

sis to follow the pre-silicon (Spice is very close to actual "physical" behavior).

Step 2. Multi-modal CPA Attacks: Leakage models (both HW and HD) are built based on the input plaintext, and both 1st- and 2nd-order attacks are performed on the masked designs. The attack order should increase for higher-order masking schemes. For example, dth-order masking schemes require up to $(d + 1)$th-order attacks. In this paper, for 1st-order masking schemes we conducted up to 2nd-order attacks. Correlation between the hypothetical power model and the collected traces is assessed using both Pearson and Spearman distinguishers as the latter performs better in some cases (refer to Sec. 3). Thus, we rely on 4 combinations of leakage models (HW and HD) and distinguishers (Pearson and Spearman) to ensure the leakage is not present when the adversary exploits any of these combinations. Attack success rate is assessed when targeting each sample point individually via N attacks on a random set of power traces. Each attack is repeated multiple times using different traces to remove the bias. Finally, security evaluation is performed on both new and the aged devices. *In this paper, we performed a total of 136 multi-modal evaluations with launching* 9.32×10^6 *attacks to show the factors affecting a CPA attack's success.*

5 Experimental Setup and Results

We implemented the first round of PRESENT cipher including the `addRoundKey` and `sBoxLayer` (also denoted S-Box) operations. GLUT, ISW, RSM, RSM-ROM, and TI masking schemes and Unprotected LUT of PRESENT S-Box are realized using 45 nm NANGATE technology. Power traces are collected from new and aged devices. Synopsys HSpice is used for transistor-level simulation. Aging impact is assessed via HSpice MOSRA Level 3 model for 10 weeks, 20 weeks, 3 years, and 6 years of operation. The time durations for aging are deliberately selected to encompass various scenarios. For instance, accelerated aging may involve waiting for a maximum feasible period of 10 or 20 weeks during operation, indicating the potential duration an attacker might bide their time. In the context of older devices, this variation can extend to 3 or 6 years, particularly when the aging impact is predominantly saturated. The simulation temperature is 105°C following grade 2 of AEC Q-100 [34, §1.3.3] considering Vdd=1.2. Power consumption samples are obtained by probing the current drawn from the Vdd source using transient analysis, with a sampling resolution of 10 ps per point. Level 5 accuracy is used in HSPICE simulations, providing high precision with 10 significant digits in the output.

For RSM and RSM-ROM (2 shares, each 4-bit) traces for 256 possible combinations are collected. 4096 traces are collected for GLUT and ISW (2 input shares + 1 output share, each 4-bit), and 65536 traces for TI (4 shares, each 4-bit). We used the same fixed key for all the traces.

CPA attacks are performed when transitioning from initial to final value during S-Box operation. *Noise-free simulated traces are used in the attacks as the goal of this study is to perform intrinsic security analysis by designer (who knows the key); thus want to simulate perfect (no-noise) glitches.* Recall that exploiting 1st-order leakage is more resilient to noise and shall be considered carefully. Hence, we have a diversity of settings during CPA. We used Pearson and Spearman correlations [29], HW and HD leakage models, and launched 1st- and 2nd-order CPAs to study the glitches in each circuit. For the 1st-order CPA, we launched multiple attacks each time targeting one sample point as the PoI. 2nd-order CPAs are done for all possible centered product combinations of sample points [27]. In each attack, to generate 10,000 traces, we randomly selected the traces out of the possible ones (e.g., 256 for RSM-ROM) so one trace can be selected multiple times. Then we explored whether the attack using 10,000 traces was successful or not. We repeated the process 1000 times to remove the bias resulting from randomly selecting the traces. Success Rates (SRs) were reported based on the average SR of these attacks. Please note that for the feasibility of pre-silicon evaluation in terms of computation time, we considered 10,000 traces as a baseline. However, designers are encouraged to select a higher or lower number of traces based on their specific needs. Increasing the number of traces can enhance the confidence level of the analysis, while reducing the number may risk missing some potential glitches; in order to miss no glitches, all transitions from arbitrary initial value to arbitrary final value shall be simulated. Therefore, we recommend selecting a number of traces that balances computational feasibility with the likelihood of capturing critical glitches.

Remark 1 *The SR is an operational leakage detection technique, because at the same it proves that there is a leakage and it exhibits the attack that exploits it. Other methods exist to detect leakage, such as the t-test, in the "Test Vector Leakage Assessment Methodology" (TVLA) paradigm. On the one hand, TVLA is less computationally demanding, but on the other hand, TVLA quantifies the leakage without though providing a distinguisher which can exploit it. Still, the two methods (SR and TVLA) are consistant in our first-order setup, as they are mathematically shown to be equivalent in [35].*

5.1 Comparing Leakage Power Models and Correlation Distinguishers Combinations in 1st-order Attacks

5.1.1 Change of PoI When Considering HW vs. HD Models

This set of results shows that the PoIs are different for different leakage power models (HW vs. HD) used in a CPA.

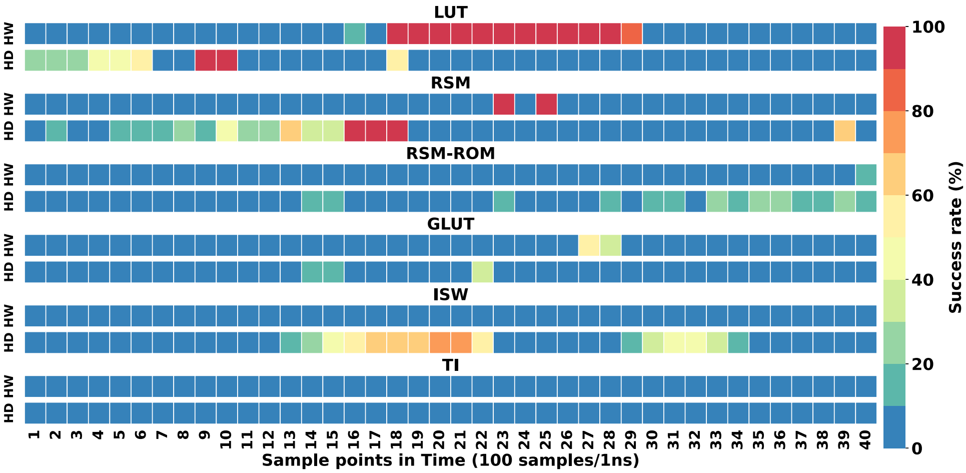

Fig. 3 Success rate's heat-map of S-Boxes for HW vs HD power models using Pearson correlation in 1st-order CPA attacks based on 10,000 traces

Figure 3 depicts the heatmap of SR of the 1st-order CPA when HW and HD power models and Pearson distinguisher were used. Attacks were performed individually for each sample point shown in X-axis. *As mentioned earlier, we focus on the multi-modal evaluation of the masking schemes so intentionally noise is not added to the traces*. The average SR is shown in each case using a color bar changing from blue (<10%) to red (>90%).

As expected and shown in Fig. 3 the unprotected LUT is more vulnerable; the graph includes more red points compared to other structures. The goal of this experiment is to analyze how the PoI changes based on the power model. As depicted LUT has more leakage when HW model is used (sample points 18 to 29) than HD model (points 9 and 10). In contrast for RSM, HD model results in more leakage than HW. Moreover, it is clearly visible that PoI changes with different power models.

The takeaway point is that in verifying the vulnerability of devices it is crucial to analyze both HW and HD power models during the CPA as one may show leakage while the other covers it. Also, the graphs show that TI is highly secure to the 1st-order attacks while ISW is vulnerable when HD model along with Pearson correlation is used. GLUT is more secure than ISW using Pearson model against 1st-order attacks.

5.1.2 Change of PoI by Using Different Distinguishers

Pearson correlation has been traditionally used in CPA attacks. However, a recent study showed that Spearman rank correlation outperforms Pearson in capturing certain non-linear leakages [29]. Figure 4 compares the SR of the attacks when each of these correlation distinguishers are used, considering HD leakage model. As shown, PoIs (which reveal glitches) change when using different distinguishers. Attack-

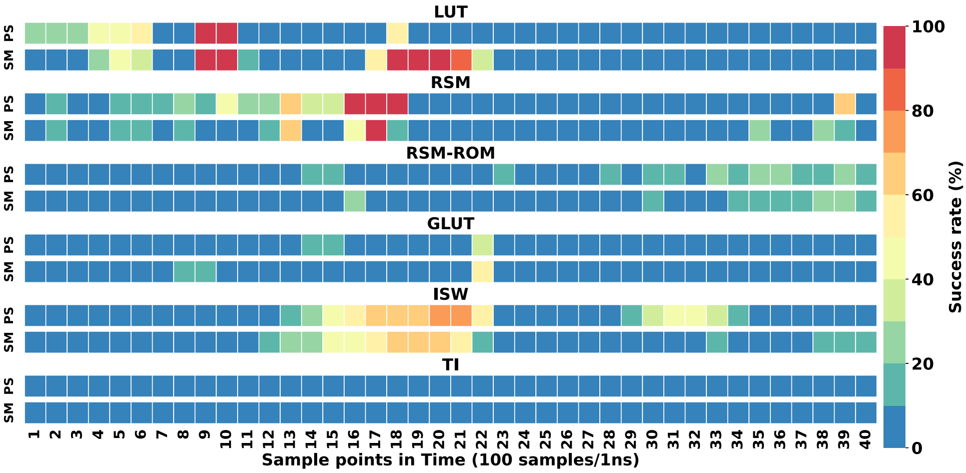

Fig. 4 Success rate's heat-map of S-Boxes for HD model using different correlation distinguishers in 1st-order CPA attack based on 10,000 traces. SM and PS refer to Spearman and Pearson distinguishers, respectively

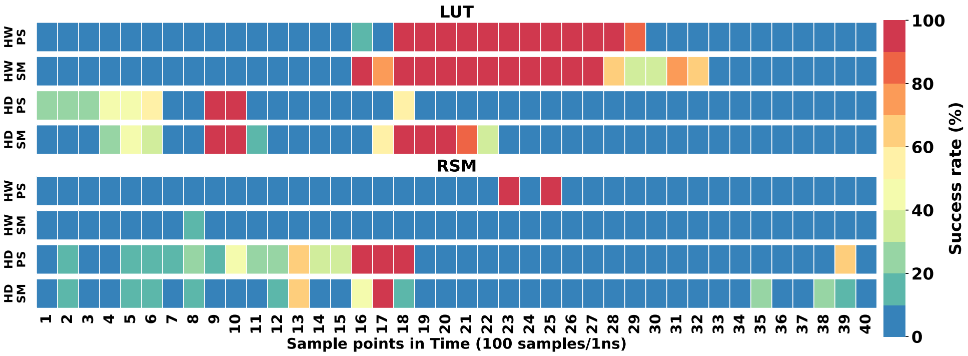

Fig. 5 Success rate's heat-map of S-Boxes for 4 categories of 1st-order CPA attacks using 10,000 traces

ing LUT was more successful when using Spearman (Sample points 17 to 22). However, for RSM, Pearson correlation benefits the adversary more. Again, among all masked circuits, RSM is the most vulnerable and TI is the most secure one. As shown the choice of a distinguisher highly affects the attack success, and it is not correct that Spearman always outperforms Pearson.

Based on the above observations, for security analysis, one should not rely on a sole distinguisher, rather he/she considers both Pearson and Spearman as one may leak the key while the other manifests the circuit secure.

5.1.3 Multi-Modal Comparison

As mentioned, both power model and distinguisher affect the selection of PoIs that reveal the glitches as well as the SR of the attacks launched on the targeted PoIs. This set of results shows the SRs of the 1st-order CPA for 4 combinations of power models and distinguishers: namely *HW-Pearson*, *HW-Spearman*, *HD-Pearson*, and *HD-Spearman*. Firstly, Fig. 5 shows the PoIs in LUT and RSM. Both circuits manifest different levels of vulnerability depending on the used power model and distinguisher. In particular, as expected, LUT can be attacked using all 4 combinations, but RSM shows more resistance with HW model. Also, Pearson distinguisher is more useful in attacking RSM than Spearman.

Figure 6 depicts the highest success rate amongst all PoIs extracted for all 4 combinations of leakage models and distinguishers. Note that in the heatmaps we only showed 40 sample points (for visibility), yet for the highest SR we considered the whole pane of their run time. The dotted line shows the SR for randomly guessing the key (4-bit). Although using the HD-Pearson seems promising in most cases, it is not always true, e.g., GLUT is different.

5.2 Effect of Aging on Leakage in 1st-order Attacks

Aging increases the delays in the circuit's paths and also alters the circuit power consumption. Thereby, it is crucial to investigate if it affects the success of the CPA attack targeting them. Figure 7 shows the SR's heatmap of the 1st-order attack when HD-Pearson is deployed to attack devices of varying ages, including new (age: 0 week), 10-week, 20-week, 3-year, and 6-year old devices. As shown in this figure, aging changes the PoIs and the attack success rate, yet the impact for the 1st-order CPA seems minor in this figure This is because aging may introduce new glitches or remove existing glitches due to the change of delays of the gates in different paths

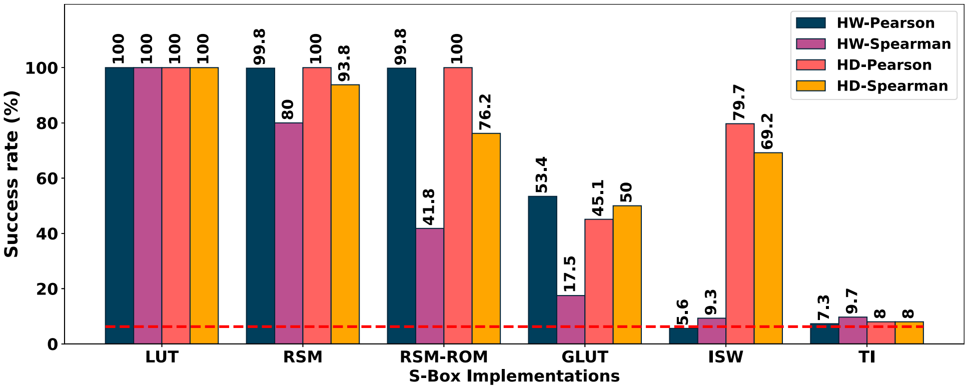

Fig. 6 Comparing S-Boxes based on the highest SR extracted from each 4 categories of 1st-order CPA attacks using 10,000 traces

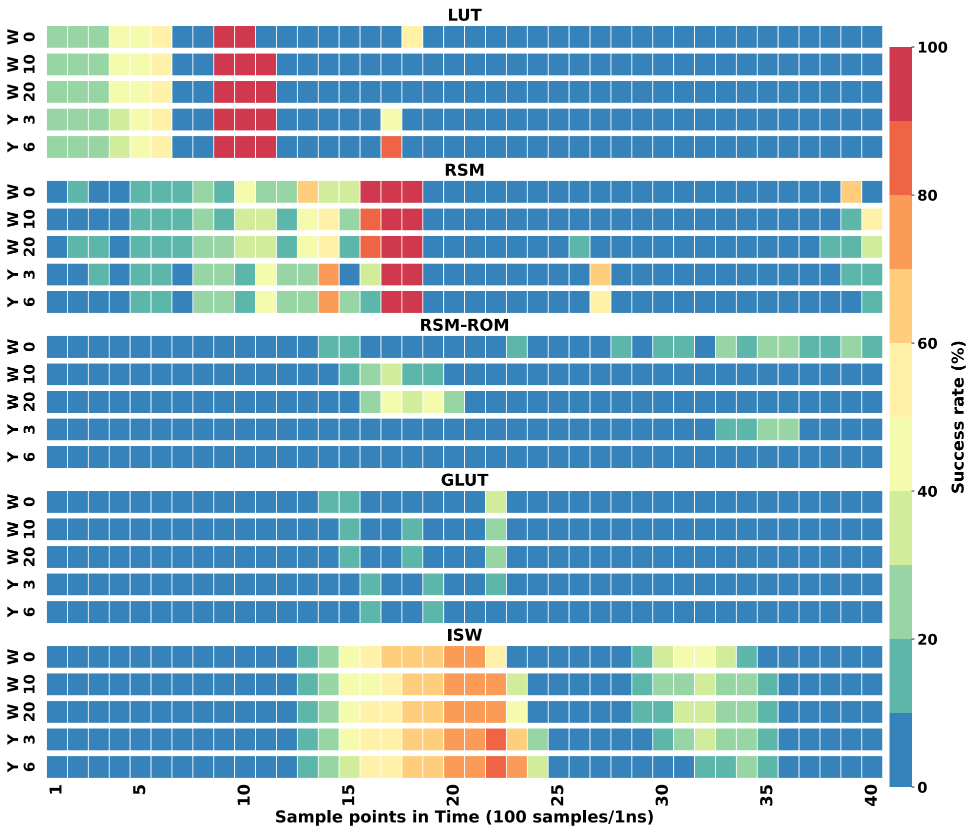

Fig. 7 Success rate's heat-map of S-Boxes in different ages when exposed to the 1st-order CPA using 10,000 traces and HD-Pearson combination

with different rates considering that aging rate of a transistor relates to its workload during the course of operation. For example, in Fig. 7, sample point 11 leaks the key in aged LUTs but not the new one (age=0). Note that although the impact of aging seems marginal in this figure when the POI is investigated, the next results show that the impact is not always minimal and the attack's SR may change significantly in some cases when the device is aged.

To investigate the aging impact on the SR of the attacks in more detail, Fig. 8 illustrates the highest success rates when attacking each circuit via CPA using 10,000 traces. TI is not shown for the sake of time as its aging simulation is highly

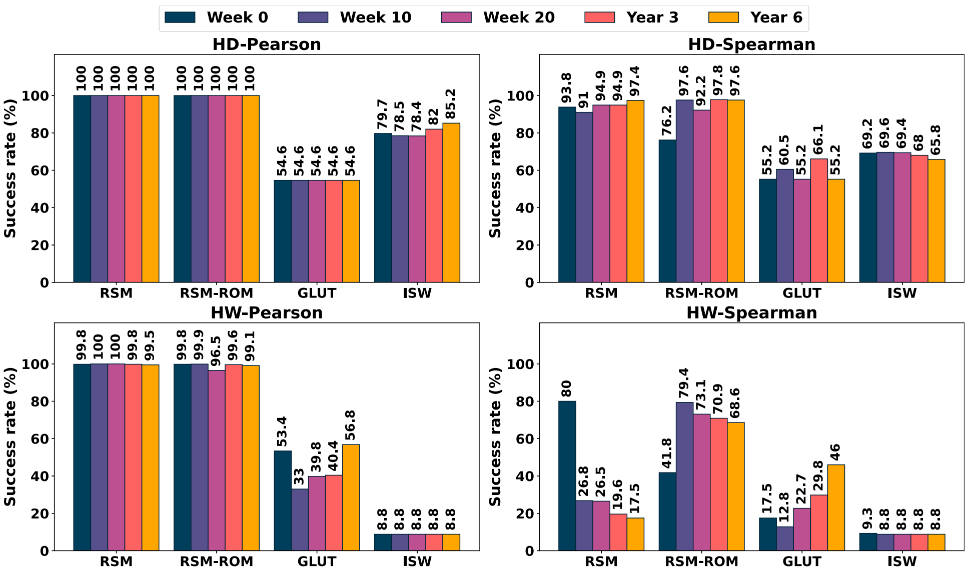

Fig. 8 Aging impact on the highest SR of 1st-order CPA using 10,000 traces for all combination

time-consuming. LUT is also excluded from the presentation since no variability is observed in its case when subjected to an attack with 10,000 traces. This is because the number of traces used exceeds the requirement for a successful attack on LUT.

The findings indicate that the influence of aging on success rates is minimal for first-order attacks when employing a Pearson distinguisher. GLUT in the case of using HW-Pearson and ISW when using HD-Pearson shows 3.4% and 5.5% increase of SR in 6 years and other cases do not show a significant change in SR when deploying Pearson distinguisher. In contrast, the Spearman distinguisher demonstrates a more significant impact due to aging on the success rates for masked devices. As illustrated, the success rate for RSM-ROM experiences an increase of up to 21.4% with HD-Spearman and 37.6% with HW-Pearson combination after 10 weeks of aging. Likewise, GLUT demonstrates an increase of up to 10.9% for HD-Spearman after 3 years and 28.5% for HW-Spearman after a 6-years. On the contrary, the aging impact could potentially enhance resiliency by diminishing the success rate in the case of RSM with the HW-Spearman combination. Indeed it indicates that the impact of aging also relies on the complexity of the masked design. For instance, ISW experiences minimal impact, whereas GLUT (style larger than ISW) is significantly affected by aging in the context of a 1st-order attack.

Interestingly, it is observed that the initial resiliency (at age 0) may diminish over time. For instance, the maximum success rate for GLUT across all combinations is 55.2% at week-0 but increased to 66.1% after 3 years of operation, particularly with the HD-Spearman combination. Likewise, for ISW employing HD-Pearson, the success rate increased from 79.7% to 85.2% after 6 years of operation.

The key takeaway from these results is that aging has the potential to modify the resiliency of a secure device. The Spearman distinguisher exhibits a greater impact on success rates with aging in the context of a 1st-order attack. *These results depict the importance and necessity of considering aging as an additional parameter for the security evaluation of critical devices.*

5.3 Multi-Modal Comparison in 2nd-Order Attacks

5.3.1 Using Different Leakage Models and Distinguishers

These results depict how the leakage model and distinguisher affect the success of a 2nd-order attack and its related PoIs. The 2nd-order attacks consider the combination of 2 sample points at a time to recover the key. Here, we consider the centered product of each 2 sample points in our attacks.

Figure 9 depicts the SR for 2nd-order attacks on RSM using 10,000 traces and 4 combinations of leakage models and distinguishers. Here, HD model seems more powerful in the attacks. The primary reason is that $HW(X)$ is a linear function on its input X, while $HD(X, Y)$ is a quadratic function on its two inputs X and Y [36, Sec. 6]. That is, when applied to attacking RSM, the HD model is capable to combine more information at higher orders. Moreover, Fig. 9 clearly shows that the higher order leakages can be exploited by both distinguishers (HD-Pearson and HD-Spearman). Another observation is that PoIs also change based on the distinguisher; similar to the 1st-order CPA. Figure 10 compares the S-Boxes against 2nd-order CPA. As shown different S-Boxes leak differently using different leakage models and distinguishers. Also, TI has 2nd-order leakage as expected.

5.3.2 Effect of Aging on 2nd-Order Attacks

As previously mentioned, power traces are impacted by aging due to changes of delay of the paths. It is crucial to analyze such aging impact on the 2nd-order attack as well. Figure 11 depicts the heat-map illustrating the effect of aging on the success rate of 2nd-order CPA, employing a combination of 10,000 traces and HD-Pearson. Similar to the 1st-order attack, the PoI undergoes changes in the 2nd-order attack, as well and might change the success rate. As an illustration, certain combinations within the [20, 25] range for both x and y axes exhibit increased strength with aging. On the contrary, combinations located between [35, 40] on the x-axis and [20, 25] on the y-axis tend to diminish with the aging impact.

Figure 12 illustrates the highest success rates of 2nd-order CPA attacks targeting masked S-Boxes across various aging conditions for all combinations. RSM and RSM-ROM are omitted since no aging variation is observed with 10,000 traces for 2nd-order CPA. TI is excluded due to the considerable time required for aging simulation.

Similar to 1st-order CPA, the results reveal that aging can have either a positive or negative impact on the success rates of 2nd-order CPA. It is observed that the Spearman distinguisher demonstrates a rising trend in success rates. As an illustration, employing HD-Spearman resulted in an increase of up to 9.5% for GLUT and 7.9% for ISW over a period of 3 years of aging. Simultaneously, there was a 6.5% increase for ISW when utilizing the HW-Spearman combination after 3 years of aging. The Pearson distinguisher exhibits both increasing and decreasing trends, depending on the specific design. For instance, with the HD-Pearson combination, GLUT experienced an increase of up to 8.1% over 3 years of aging, whereas ISW's success rate decreased by up to 16% over a 6-year aging period. Likewise, for ISW with the HW-Pearson combination, the success rate increases by up to 10% after 20 weeks of aging, but it decreases significantly by 40.7% after 6 years of operation.

The key takeaway from these observations is that aging has an impact on the success rates for 2nd-order CPA, influencing them either positively or negatively. Consequently, these

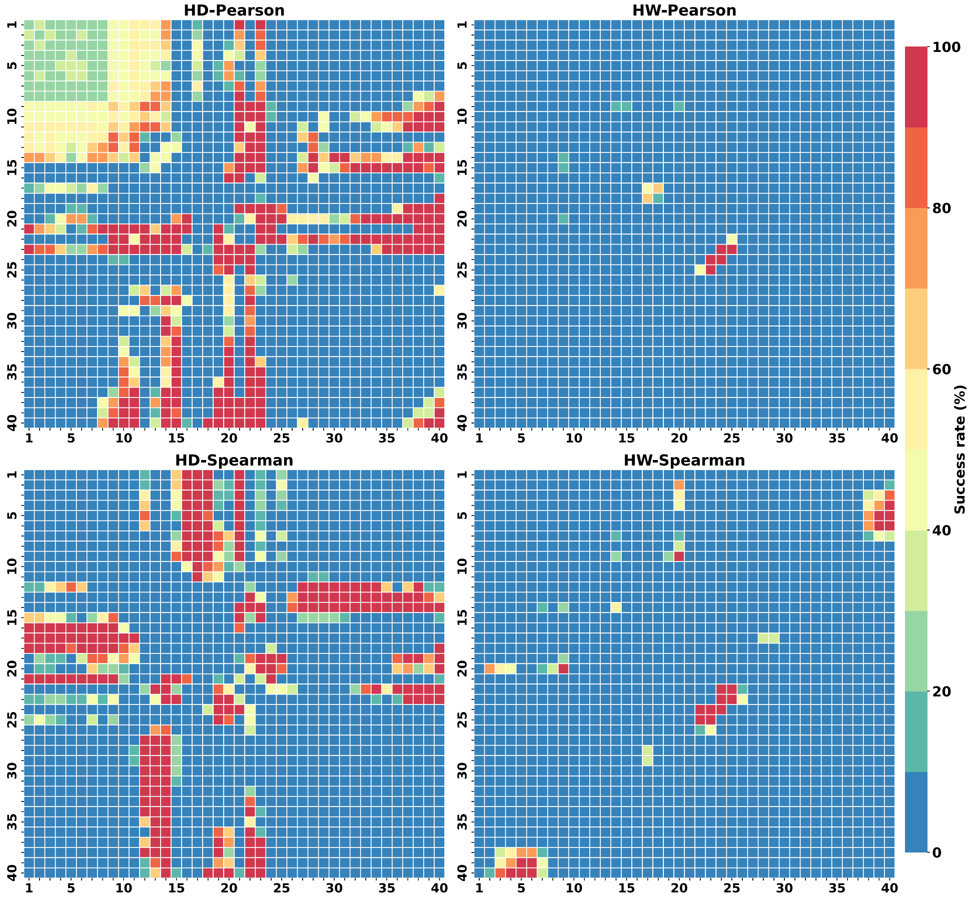

Fig. 9 Success rate's heatmap for 4 combinations of distinguisher and power model used for the 2nd-Order CPA attacks on RSM via 10,000 traces

results highlight the importance of assessing the resiliency of a masked device under aging conditions during the pre-silicon evaluation.

5.4 Effect of PoI Selection in CPAs against Masked S-Boxes

As discussed in Sec. 3, the adversary may use the PoI selection methods to increase the probability of the attack success. As in this paper we focus on pre-silicon security analysis by the designer, we consider every sample point as the PoI and launch several attacks as shown in Figs. 3, 4, 5, 6, 7, 8, 9, 10, 11 and 12. However, to show what the adversary achieves when using the state-of-the-art PoI selection methods, we used SOST and launched the 1st-order CPA attacks based on the PoIs those SOST reveals.

To show the importance of our proposal in verifying the security of the design via attacking each sample point individually, we compare our results with the case SOST PoI selection is used. The latter is shown in Fig. 13 depicting the SR of the 1st-order CPA when selecting 10 PoIs with maximum SOST indexes. Comparing these results with Fig. 6

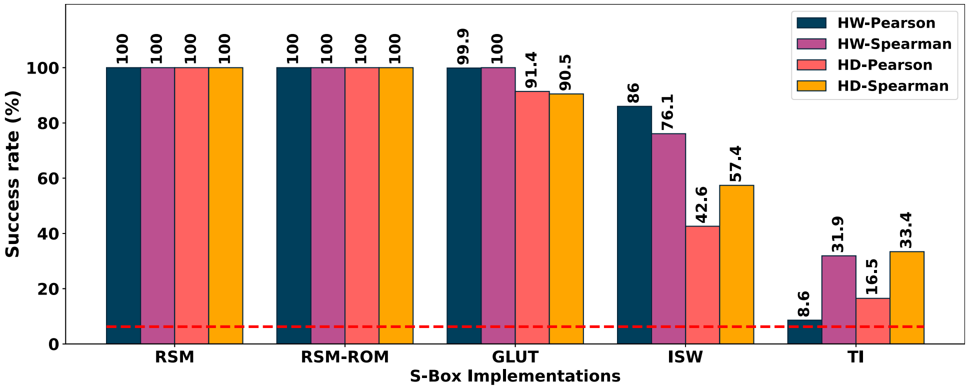

Fig. 10 Comparing S-Boxes based on the highest SR extracted from each 4 categories of 2nd-order CPA attacks using 10,000 traces

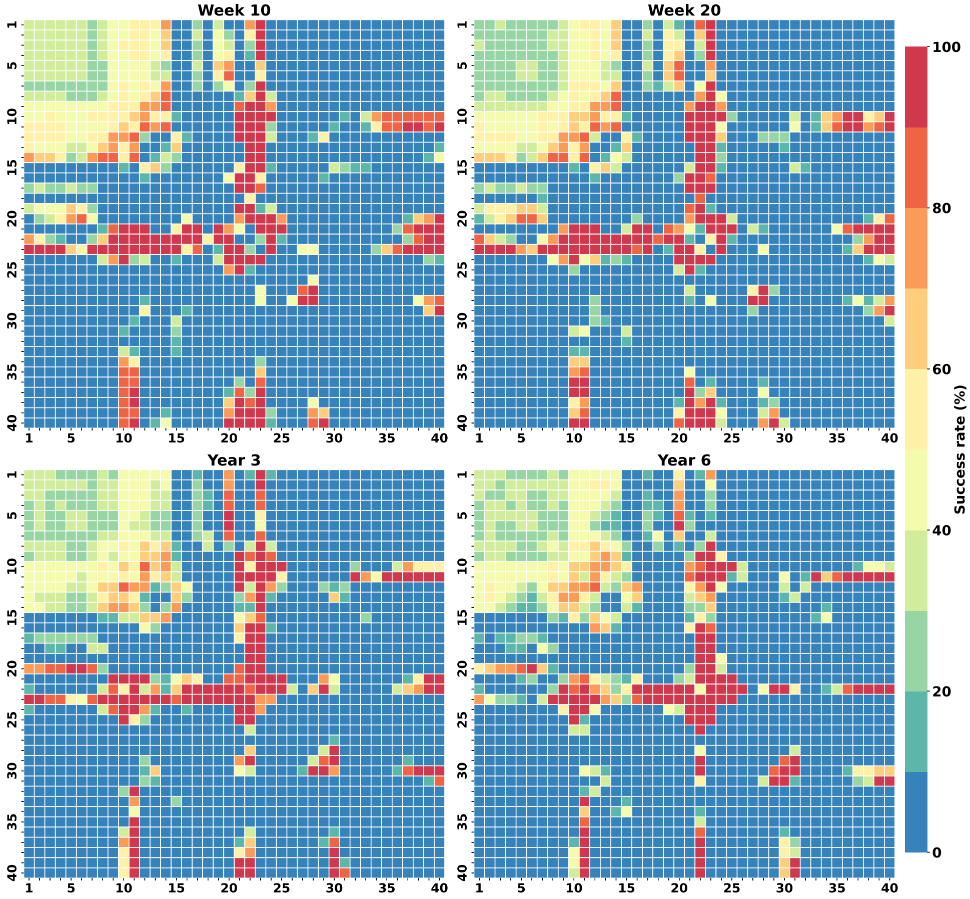

Fig. 11 Success rate's heat-map of RSM S-Box in different ages when exposed to the 2nd-order CPA using 10,000 traces and HD-Pearson combination

clearly shows that such PoI selection is not appropriate. For example, RSM cannot be attacked using HW model when using SOST while it was shown to be vulnerable in Fig. 6.

We also performed 2nd-order CPA using MIA [31] PoI selection method. Similar results (no success in the attacks based on the MIA PoIs) were achieved yet not shown for the sake of

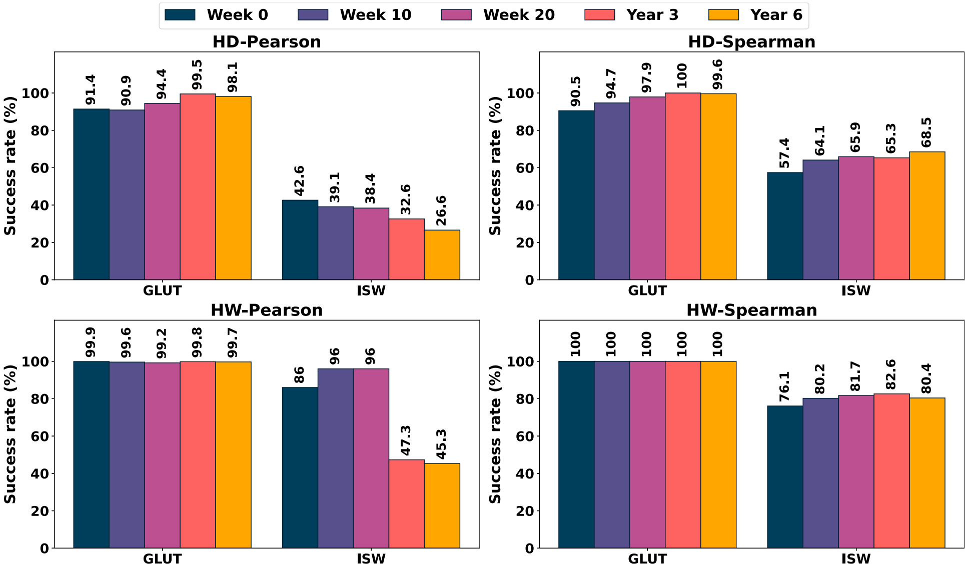

Fig. 12 Effect of Aging on 2nd-order attack using 10,000 traces. RSM and RSM-ROM are not shown as no aging variation is observed using 10,000 traces for 2nd-order CPA. TI is not shown for the sake of its time for aging simulation

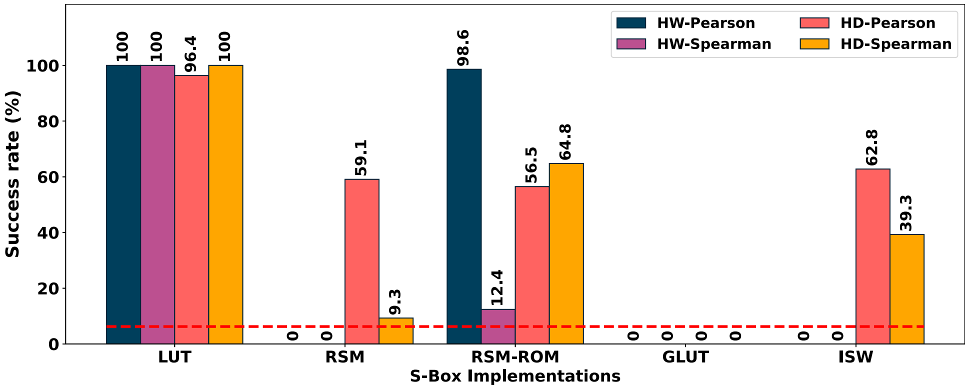

Fig. 13 SR for 1st-order CPA on 10 points with max SOST indexes. TI is not shown as it is not attackable by 1st-order CPA (recall Fig. 6)

space. *The takeaway is that PoI selection might not be effective for masked circuits as PoI changes based on the leakage model and distinguisher. Thus, relying on these methods and attacking based on those PoIs may not reveal the security flaws in the pre-silicon*. Thus, we urge the designer not to limit the security analysis to the PoIs selected by these state-of-the-art methods.

5.5 Comparison Among Masking Styles

Table 2 summarizes the results presented above on the worst-case vulnerability corners (best case for the attack) for the targeted circuits. Here we show the worst-case scenario occurs for different combinations of leakage model and distinguisher in the targeted styles. This implies that neglecting certain corners during security assessments may result in overlooking potential sources of leakage. Furthermore, we note that 2nd-order attacks exhibit greater potency when compared to 1st-order attacks, and standardized PoI selection strategies such as SOST and MIA did not contribute to identifying the most optimal leakage from the acquired traces.

Next set of results compares the masking schemes according to both the security they offer and their PPA in different aging conditions. Instead of Power consumption we show the total energy consumption as the total number of points selected for attacking different circuits can be different based on their timing. For the security, we compare the highest SR an attacker can achieve in different aging conditions for different pairs of leakage model and distinguisher for the 1st-order leakage as in practice 2nd-order CPA is considered a *residual threat* which becomes marginally relevant as SNR increases.

Figure 14 shows the results for 10,000 traces at different ages: the higher the SR, the more vulnerable the circuit. As observed ISW and GLUT offer good protection with moderate energy usage, while TI provides the highest level of security but at the cost of consuming higher energy. In terms of performance, TI demonstrated superiority over other styles, whereas RSM-ROM fell short of delivering the anticipated security, even with a higher timing cost. From the area perspective, LUT offers minimal security with the smallest area, as expected, yet not secure. However, RSM and RSM-ROM are found to be the most vulnerable options even with the cost of higher area. ISW implies the lowest area yet with the cost of security loss compared to GLUT which is shown as a good choice considering balance between the cost of security and area. TI is proven to be the best secure masking style with the cost of highest area as expected. The takeaway is that the higher security is achieved with higher area. TI is still vulnerable to 2nd-order CPA (Fig. 10) yet better protection than other masking schemes. This comparative analysis of trade-offs will help designers in selecting the most suitable masking style according to their specific requirements and budget.

As observed from the Fig. 14 it is evident that aging has led to changes in the success rate over time. Furthermore, there is an average decrease in energy consumption, while the maximum delay of the devices shows an increase. However, as shown in this figure, although the security of

Table 2 Worst-case vulnerability corners for different masked S-Boxes

S-Box	Power Model	Distinguisher	Attack Order	PoI Sel. Helped?
LUT	HW	Spearman	1st	NO
RSM	HD	Pearson	2nd	NO
RSM-ROM	HD	Pearson	2nd	NO
GLUT	HW	Pearson	2nd	NO
ISW	HW	Pearson	2nd	NO
TI	HD	Spearman	2nd	NO

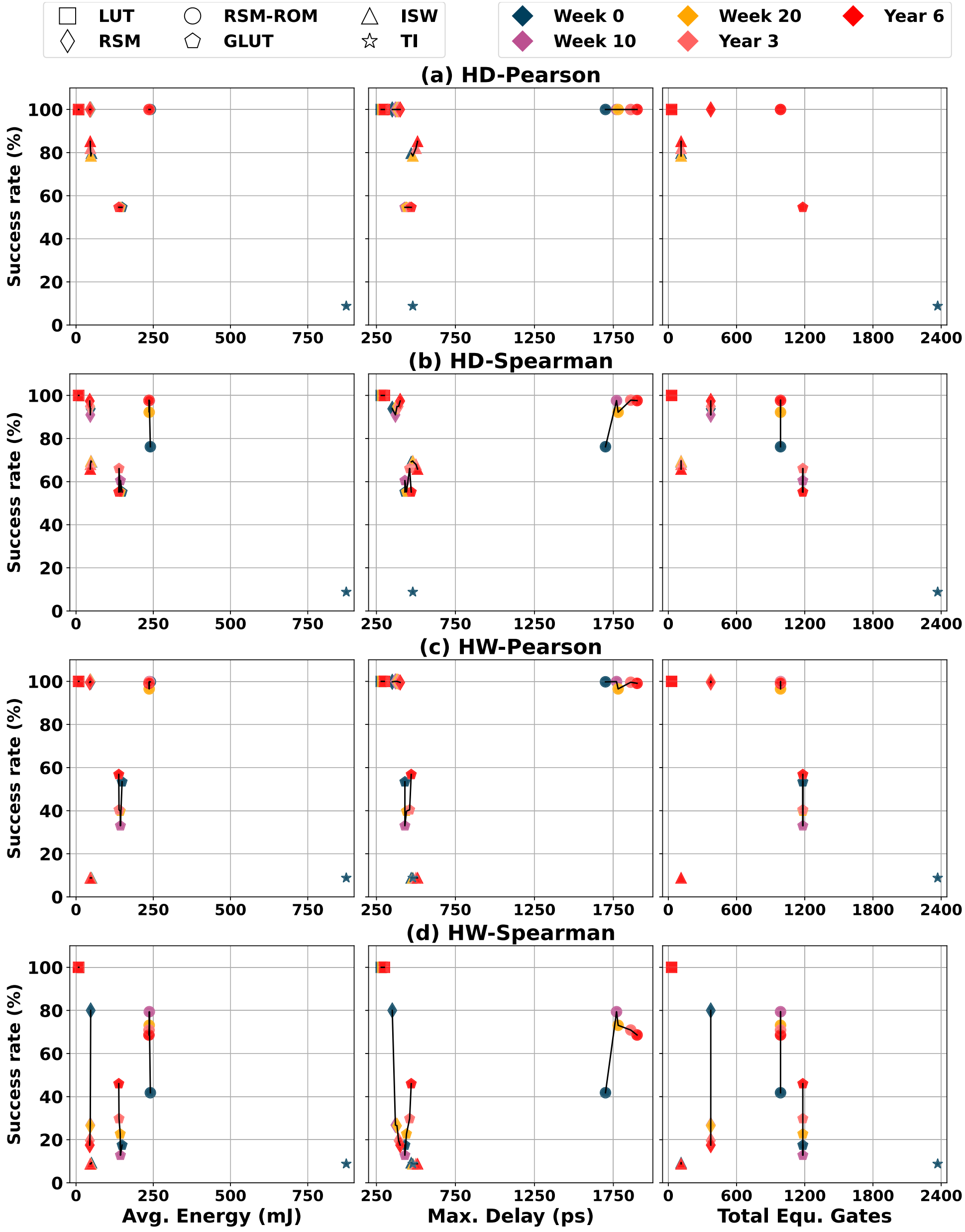

Fig. 14 PPA vs. security in new and aged devices for 4 combinations of leakage models & distinguishers. Masking styles are represented by distinct marker shapes, while ages are distinguished using different colors. Here the security is shown via the highest SR of the 1st-order CPAs in different aging (the higher the SR the lower the security). TI is omitted from the aged device results due to its extensive aging simulation time

each circuit changed over time (slightly in this figure due to resolution but more observable in previous figures showing the aging impacts) the relative security of the considered masking schemes did not change over time, e.g., GLUT has the highest security among all considered masking schemes (except TI for which due to the very long aging simulation time we did not show it. We expect that TI remains as the most secure after aging as well.) This analysis of security versus PPA under aging conditions highlights how aging can impact the security of a device across various leakage models and distinguishers. This aids designers or security verifiers in forecasting the security level of a system as the device ages. It enables them to select the appropriate masking style based on the PPA trade-off, ensuring sustained security even as the device undergoes aging.

Figure 14 provided a comprehensive analysis for designers to choose a masking style based on Security vs. PPA considerations. The goal of this experiment is to both summarize the findings from Fig. 14 and verify the relative security offered by each masking scheme. In this respect, Fig. 15 presents the *maximum success rate* across all combinations of leakage models and distinguishers, and aging conditions providing a measure of overall security in the worst-case scenario. This approach offers a security estimation that accounts for all parameter shifts presenting maximum vulnerability the design can face during its lifetime.

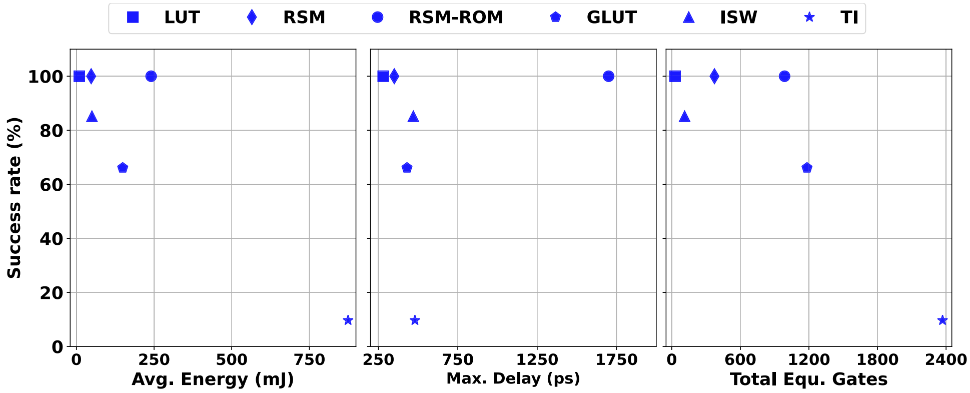

Fig. 15 Overview of area versus security of masked devices considering the maximum success rate across all combinations of leakage models, distinguishers and aging conditions

The objective of this experiment is to determine the optimal masked design that best aligns with the designer's specific requirements. Thus Fig. 15 portrays the various masking styles along with their overall security vs. PPA trade-offs. As expected, the unprotected LUT is the weakest in terms of security, while TI provides the highest security. However, TI comes with the significant drawback of high power consumption and large area overhead. It is understandable that reducing these overheads might be necessary depending on the desired level of security.

The aim is to minimize both the x-axis (PPA) and y-axis (success rate) values. It was found that the ISW masking style offers lower power consumption but is more vulnerable to attacks, whereas GLUT strikes a balance between power consumption and security. Performance-wise, considering maximum delay, GLUT also proves to be the most suitable choice. In terms of the area versus security trade-off, ISW is preferred due to its minimal area requirement among the compared masking styles. However, to achieve higher security, one may need to accept greater area overhead and opt for GLUT, which balances security and area overhead. These analyses provide valuable guidance for designers in selecting the optimal masked design based on specific requirements.

The key takeaway from this experiment is that evaluating the worst-case scenario across all parameter combinations provides a comprehensive summary of a design's overall vulnerability. By considering this vulnerability in conjunction with the PPA graph, designers can make informed decisions to select the most suitable design based on their specific needs.

6 Discussion

Among different attack parameters, our analysis reveals the crucial role of PoIs. We find that on "ideal traces" (captured noiseless from Spice), poorly selection of PoIs results in some attack failure despite the implementation is otherwise attackable by keeping all time samples in the list of PoIs. Thereby, PoIs selection can be deceptive and mislead security judgment of the studied countermeasure. The crucial finding here is that using the state-of-the-art PoI selection such as SOST and MIA can be misleading and relying on them during the pre-silicon analysis can result in chips with security flaws.

We observed that masked circuit often produce glitches that are difficult to detect using conventional PoI selections, like SOST and MIA). Therefore, we recommend selecting PoI sample points across the entire targeted clock cycles. For instance, in this analysis, we considered a 500ps clock cycle, with most operations completing by 400ps. However, it is crucial to include the 400ps to 500ps interval due to potential delays caused by aging degradation.

It is also mandatory to perform attacks assuming both *activity-based* leakage model (e.g., HD) and *value-based* leakage model (e.g., HW). Even though glitches are physically arising from spurious activity, we see that some logic styles can feature a leakage based on value (maybe owing to the gates where leakage depending on the value of the still inputs, as per [37]). This is also a crucial finding as per [14], it has been recommenced to focus on HD than HW, yet as we showed we cannot only rely on HD models in pre-silicon security analysis. Therefore, we recommend utilizing both HW and HD model during pre-silicon security analysis.

Regarding the distinguishers, although Spearman is seen advantageous compared to Pearson, in the context of detecting "hard to model" glitches (it can admittedly be viewed as *disruptive* in the baseline leakage model), it is not always the most successful distinguisher, as cannot supersede Pearson. We recommend conducting analysis using both Pearson and Spearman distinguishers, as it is difficult to determine which is more effective across varying parameters and design types. This ensures that no advantage is given to adversaries by their choice of distinguisher.

The aging in general has a strong impact: either negatively on template attacks (if model and attack traces have aging misalignments) [38], or positively when acting on hiding countermeasures (e.g., dual-rail logic, which gets more unbalanced over time) [39]. But in the case of CPA on masked circuits, we find that aging can have positive or negative impact on the attack success when different distinguishers and/or leakage models are used, i.e., if the adversary uses Spearman distinguisher in most cases the SR that is achieved when targeting an aged device is higher than when attacking the new one.

Finally, we show that all logic styles (incl. TI – see Fig. 10) are vulnerable to 2nd-order attacks. These observations verify our analysis as indeed all masking schemes we studied only claim 1st-order security. But comparing 1st-order vs 2nd-order (Fig. 6 vs Fig. 10) reveals that success rates for 10,000 traces are comparable, in the absence of noise. Thus, when the measurement noise increases, the 1st-order attacks will become prevalent compared to 2nd-order. It is therefore mostly important to analyze 1st-order masking schemes.

Furthermore, designers can perform a comprehensive analysis of masking styles based on Security versus PPA considerations using the framework presented in Fig. 2. Such an analysis can be visualized similarly to Fig. 14 to aid designers in their decision-making process. Ultimately, determining the optimal masked design that aligns with the designer's specific requirements involves evaluating the worst-case scenario across all parameter combinations. By considering this vulnerability alongside the PPA graph, as shown in Fig. 15, designers can make informed decisions.

7 Conclusion

Pre-silicon security analysis is performed to characterize the expected resiliency of the chip against attacks before fabrication. However, the previous work in this area is mainly fragmented in case that only few of the factors affecting the success of an attack is considered during such pre-silicon analysis. This paper first showed how considering the combination of these factors (leakage model, distinguisher, PoI selection, etc) can affect the analysis and prevent approving the designs with security flaws pre-silicon. We also investigated the aging impacts on the success of the CPA attacks on masked circuits and showed that the success may increase or decrease over the course of aging but the aging impact cannot be ignored during the pre-silicon analysis of security as aging impacts on the attack success changes from one distinguisher and leakage model to another and thus an aged device may be more resilient compared to a new one when exposed to a specific distinguisher and leakage model but more fragile when another distinguisher or leakage model is used by the adversary. We also comparatively studied 5 state-of-the-art masking schemes in terms of security versus PPA. Such analysis enables the designers to select the appropriate countermeasure based on the security budgets and design constraints.

Acknowledgements This research has been supported in part by the National Science Foundation CAREER Award (NSF CNS-1943224). We acknowledge another funding by the bilateral French-German "APRIORI" project (ANR-20-CYAL-0007, MESRI-BMBF call).

Data Availability All data generated or analyzed during this study are within the paper.

Declarations

Conflicts of Interest The authors declare that they have no conflict of interest.

References

1. Picek S, Perin G, Mariot L, Wu L, Batina L (2023) Sok: Deep learning-based physical side-channel analysis. ACM Comput Surveys 55(11):1–35
2. Prouff E, Rivain M (2007) A Generic Method for Secure SBox Implementation. In: International Workshop on Information Security Applications, pp 227–244 . Springer
3. Nassar M, Souissi Y, Guilley S, Danger J-L (2012) RSM: A Small and Fast Countermeasure for AES, Secure against 1st and 2nd-order Zero-offset SCAs. In: 2012 Design, Automation & Test in Europe Conference & Exhibition (DATE), pp 1173–1178 . IEEE
4. Giaconia M, Macchetti M, Regazzoni F, Schramm K (2007) Area and Power Efficient Synthesis of DPA-Resistant Cryptographic S-Boxes. In: 20th International Conference on VLSI Design, pp 731–737. IEEE Computer Society, Bangalore, India
5. Ishai Y, Sahai A, Wagner D (2003) Private Circuits: Securing Hardware against Probing Attacks. In: Advances in Cryptology-CRYPTO 2003: 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, 17-21 August, 2003. Proceed 23, vol 2729, pp 463–481
6. Nikova S, Rijmen V, Schläffer M (2008) Secure Hardware Implementation of Non-linear Functions in the Presence of Glitches. In: Information Security and Cryptology – ICISC, vol 5461, pp 218–234. Springer, Seoul, Korea
7. Groß H, Mangard S, Korak T (2016) Domain-Oriented Masking: Compact Masked Hardware Implementations with Arbitrary Protection Order. In: Cryptology ePrint Archive 2016, p 3
8. Cassiers G, Grégoire B, Levi I, Standaert F (2021) Hardware Private Circuits: From Trivial Composition to Full Verification. IEEE Trans Comput 70(10):1677–1690
9. Chaves R, Chmielewski Ł, Regazzoni F, Batina L (2018) SCA-Resistance for AES: How Cheap Can We Go? In: Progress in Cryptology–AFRICACRYPT 2018: 10th International Conference

on Cryptology in Africa, Marrakesh, Morocco, 7–9 May, 2018, Proceed 10, pp 107–123 . Springer

10. Mangard S, Popp T, Gammel BM (2005) Side-Channel Leakage of Masked CMOS Gates. In: Cryptographers' Track at the RSA Conference, vol 3376, pp 351–365
11. Mangard S, Schramm K (2006) Pinpointing the Side-Channel Leakage of Masked AES Hardware Implementations. In: International Workshop on Cryptographic Hardware and Embedded Systems, pp 76–90 . Springer
12. Liu H, Qian G, Tsunoo Y, Goto S (2011) The Switching Glitch Power Leakage Model. J Softw (JSW) 6(9):1787–1794. Academy Publisher
13. Bruneau N, Guilley S, Najm Z, Teglia Y (2018) Multivariate high-order attacks of shuffled tables recomputation. J Cryptology 31(2):351–393
14. Balasch J, Gierlichs B, Grosso V, Reparaz O, Standaert F (2014) On the Cost of Lazy Engineering for Masked Software Implementations. In: Smart Card Research and Advanced Applications - 13th International Conference, CARDIS 2014, Paris, France, 5-7 November, 2014. Revised Selected Papers, pp 64–81
15. Goodwill G, Jun B, Jaffe J, Rohatgi P (2011) A testing methodology for side-channel resistance validation. NIST Non-Invasive Attack Testing Workshop
16. Bahrami J, Ebrahimabadi M, Danger J, Guilley S, Karimi N (2022) Leakage Power Analysis in Different S-Box Masking Protection Schemes. In: Design, Automation & Test in Europe Conference & Exhibition, DATE, Antwerp, Belgium, pp 1263–1268
17. Eurosmart (2021) Secure Sub-System in System-on-Chip (3S in SoC) Protection Profile (PP 0117)
18. Federal Office for Information Security (BSI) (2022) Certification Report V1.1 CC-PP-414 V3.6, of Common Criteria Protection Profile BSI-CC-PP-0117-2022 [Secure Sub-System in System-on-Chip (3S in SoC)], version 1.5. valid until 28 February 2032
19. Li H, Wu K, Yu F, Yuan H (2010) Evaluation Metrics of Physical Non-invasive Security. In: 4th IFIP WG 11.2 International Workshop, WISTP. Lect Note Comput Sci, vol 6033, pp 60–75. Springer, Passau, Germany
20. Nassar M, Guilley S, Danger J-L (2011) Formal Analysis of the Entropy / Security Trade-off in First-Order Masking Countermeasures against Side-Channel Attacks. In: International Conference on Cryptology in India, pp 22–39
21. Carlet C, Guilley S (2013) Side-channel indistinguishability. In: Lee RB, Shi W (eds.) Proceedings of the 2nd International Workshop on Hardware and Architectural Support for Security and Privacy, p 9
22. Covic A, Ganji F, Forte D (2020) Circuit masking schemes: New hope for backside probing countermeasures? SRC TECHCON
23. Courtois N, Hulme D, Mourouzis T (2011) Solving Circuit Optimisation Problems in Cryptography and Cryptanalysis. IACR Cryptology ePrint Archive, 475
24. Roy DB, Bhasin S, Guilley S, Heuser A, Patranabis S, Mukhopadhyay D (2018) CC meets FIPS: A hybrid test methodology for first order side channel analysis. IEEE Trans Comput 68(3):347–361
25. Nikova S, Rechberger C, Rijmen V (2006) Threshold Implementations Against Side-Channel Attacks and Glitches. International Conference on Information and Communications Security, vol 4307. LNCS. Springer, Raleigh, NC, USA, pp 529–545
26. Mangard S, Oswald E, Popp T (2006) Power Analysis Attacks: Revealing the Secrets of Smart Cards. Springer, Secaucus, NJ, USA, p 338
27. Prouff E, Rivain M, Bevan R (2009) Statistical Analysis of Second Order Differential Power Analysis. IEEE Trans Comput 58(6):799–811
28. Brier É, Clavier C, Olivier F (2004) Correlation power analysis with a leakage model. In: Cryptographic Hardware and Embedded Systems-CHES 2004: 6th International Workshop Cambridge, MA, USA, 11-13 August, 2004. Proceed 6, pp 16–29
29. Batina L, Gierlichs B, Lemke-Rust K (2008) Comparative Evaluation of Rank Correlation Based DPA on an AES Prototype Chip. International Conference on Information Security, vol 5222. Lecture Notes in Computer Science. Springer, Taipei, Taiwan, pp 341–354
30. Gierlichs B, Lemke-Rust K, Paar C (2006) Templates vs. stochastic methods: A performance analysis for side channel cryptanalysis. In: Cryptographic Hardware and Embedded Systems-CHES 2006: 8th International Workshop, Yokohama, Japan, 10-13 October, 2006. Proceed 8. LNCS, vol 4249, pp 15–29
31. Reparaz O, Gierlichs B, Verbauwhede I (2012) Selecting Time Samples for Multivariate DPA Attacks. In: Cryptographic Hardware and Embedded Systems–CHES 2012: 14th International Workshop, Leuven, Belgium, 9-12 September, 2012. Proceed 14, pp 155–174
32. Fadaeinia B, Anik MTH, Karimi N, Moradi A (2021) Masked SABL: A Long Lasting Side-Channel Protection Design Methodology. IEEE Access 9:90455–90464
33. Anik MTH, Guilley S, Danger J-L, Karimi N (2020) On the effect of aging on digital sensors. In: VLSID, pp 189–194
34. Automotive Electronics Council (2007) AEC-Q100. Failure Mechanism Based Stress Test Qualification For Integrated Circuits, Rev-G
35. Roy DB, Bhasin S, Guilley S, Heuser A, Patranabis S, Mukhopadhyay D (2019) CC meets FIPS: A hybrid test methodology for first order side channel analysis. IEEE Trans Comput 68(3):347–361
36. Cheng W, Guilley S, Carlet C, Danger J, Mesnager S (2021) Information Leakages in Code-based Masking: A Unified Quantification Approach. IACR Trans Cryptogr Hardw Embed Syst 2021(3):465–495
37. Sugawara T, Suzuki D, Saeki M, Shiozaki M, Fujino T (2013) On Measurable Side-Channel Leaks Inside ASIC Design Primitives. In: Cryptographic Hardware and Embedded Systems (CHES), pp 159–178
38. Niknia F, Danger J-L, Guilley S, Karimi N (2022) Aging effects on template attacks launched on dual-rail protected chips. IEEE Trans Comput-Aided Design of Integ Circ Syst 41(5):1276–1289
39. Anik MTH, Fadaeinia B, Moradi A, Karimi N (2021) On the Impact of Aging on Power Analysis Attacks Targeting Power-Equalized Cryptographic Circuits. In: Proceedings of the 26th Asia and South Pacific Design Automation Conference, pp 414–420

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Md Toufiq Hasan Anik received the B.Sc. degree in Electrical and Electronics Engineering from BRAC University, Bangladesh in 2016. He completed his M.Sc. degree in Computer Engineering at University of Maryland Baltimore County (UMBC) in 2023. He is currently a Ph.D. candidate in Computer Engineering at UMBC. He worked at Intel as a Computer Architecture Graduate Intern during summer 2021 & 2022. Also, as a Security Researcher Intern during summer 2020. He has authored/co-authored more than 13 papers in referred conference proceedings and journal manuscripts. His research interest includes hardware security and in particular, power analysis attacks and countermeasures, as well as sensor-assisted secure and reliable design. He conducts research in the SECure, REliable and Trusted Systems (SECRETS) research lab at UMBC.

Hasin Ishraq Reefat received his B.Sc. degree in Electrical and Electronics Engineering from Bangladesh University of Engineering and Technology (BUET) in 2021. He is currently a Ph.D. student in Computer Engineering at the University of Maryland, Baltimore County (UMBC), working in the SECure, REliable and Trusted Systems (SECRETS) research lab. His research focuses on hardware security, encompassing areas such as side-channel analysis, sensor-based security and reliability design, authentication and secure communication protocols for the IoT networks.

Wei Cheng received the Ph.D. degree in information and communications from Télécom Paris, Institut Polytechnique de Paris, France, in 2021. He is currently a Post-Doctoral Researcher at Secure-IC S.A.S., and also an (invited) Associate Researcher at Télécom Paris. His research interests include information theory, side- channel analysis, related countermeasures (mainly on code-based masking, including inner product masking, direct sum masking, polynomial masking, and other variants) for embedded systems, and secure cryptographic implementations. He also works on machine learning-based analysis on physical unclonable functions (PUFs).

Jean-Luc Danger is full Professor at TELECOM Paris. He is the head of the digital electronic system research team involved in Research in security/safety of embedded systems, configurable architectures, and implementation of complex algorithms in ASICs or FPGAs. He authored more than 250+ scientific publications and patents in architectures of embedded systems and security. He received his engineering degree in Electrical Engineering from É cole Supérieure d'É lectricité in 1981. After 12 years in industrial laboratories (namely PHILIPS, NOKIA), he joined TELECOM Paris in 1993 where he became full professor in 2002. He is a co-founder of Secure-IC. His personal research interests are trusted computing in embedded systems, random number generation, and protected implementations in novel technologies.

Sylvain Guilley is General Manager and Chief Technology Officer at Secure-IC, a company offering security for embedded systems. Secure-IC's flagship technology is the multi-certified Securyzr™ integrated Secure Element (iSE). Within Secure-IC, he is also director of "Threat Analysis" and "Think Ahead" business lines, which develop respectively security evaluation tools and advanced research. Sylvain is also professor at TELECOM-Paris, associate research at É cole Normale Supérieure (ENS), and adjunct professor at the Chinese Academy of Sciences (CAS). His research interests are trusted computing, cyber-physical security, secure prototyping in FPGA and ASIC, and formal/mathematical methods. Since 2012, he organizes the PROOFS workshop, which brings together researchers whose objective is to increase the trust in the security of embedded systems. He is also lead editor of international standards, such as ISO/IEC 20897 (Physically Unclonable Functions), ISO/IEC 20085 (Calibration of non-invasive testing tools), ISO/IEC 24485 (White Box Cryptography), and ISO/IEC 17825 (detection of side-channel leakage). He is "High Level Principles for Design/Architecture" team leader for the drafting of Singapore TR68-3 standard on Cyber-Security of Autonomous Vehicles. Sylvain is associate editor of the Journal of Cryptography Engineering (JCEN, Springer). He has coauthored 300+ research papers and filed 40+ patents. He is member of the IACR and senior member of the IEEE and of the CryptArchi club. He is an alumni of Ecole Polytechnique and TELECOM-ParisTech.

Naghmeh Karimi received the B.Sc., M.Sc., and Ph.D. degrees in Computer Engineering from the University of Tehran, Iran in 1997, 2002, and 2010, respectively. She was a visiting researcher at Yale University, USA between 2007 and 2009, and a post-doctoral researcher at Duke University, USA during 2011-2012. She has been a visiting assistant professor at New York University and Rutgers University between 2012 and 2016. She joined University of Maryland Baltimore County in 2017 where she is an Associate Professor and leads the SECure, REliable and Trusted Systems (SECRETS) research lab. She has published three book chapters and authored/co-authored over 100 papers in referred conference proceedings and journal manuscripts. She serves as an Associate Editor of the Springer Journal of Electronic Testing: Theory and Applications (JETTA) and IEEE Design & Test Journal. She has been the corresponding guest editor of the Journal on Emerging and Selected Topics in Circuits and Systems (JETCAS); special issue in Hardware Security in Emerging Technologies in 2021. Her current research interests include hardware security, VLSI testing, design-for-trust, design-for-testability, and design-for-reliability. She is a recipient of the National Science Foundation CAREER Award in 2020.

Authors and Affiliations

Md Toufiq Hasan Anik[1] · **Hasin Ishraq Reefat**[1] · **Wei Cheng**[2,3] · **Jean-Luc Danger**[2] · **Sylvain Guilley**[2,3] · **Naghmeh Karimi**[1]

Hasin Ishraq Reefat
hasinishraq@umbc.edu

Wei Cheng
wei.cheng@telecom-paris.fr

Jean-Luc Danger
jean-luc.danger@telecom-paris.fr

Sylvain Guilley
sylvain.guilley@secure-ic.com

Naghmeh Karimi
nkarimi@umbc.edu

[1] CSEE, University of Maryland Baltimore County, Baltimore, Maryland, USA

[2] LTCI, Télécom Paris, Institut Polytechnique de Paris, Palaiseau, France

[3] Secure-IC S.A.S., Paris, France