Aging Effects on Template Attacks Launched on Dual-Rail Protected Chips

Farzad Niknia, *Student Member, IEEE*, Jean-Luc Danger, *Member, IEEE*, Sylvain Guilley, *Member, IEEE*, and Naghmeh Karimi, *Member, IEEE*

***Abstract*—Profiling side-channel attacks in which an adversary creates a "profile" of a sensitive device and uses such a profile to model a target device with similar implementation has received the lion's share of attention in the recent years. In particular, template attacks are known to be the most powerful profiling side-channel attacks from an information theoretic point of view. When launching such an attack, the adversary first builds a model based on the leakage of the profiling (training) device in his disposal, which is then exploited in the second phase of the attack (i.e., matching) to extract the key from the target device. Discrepancies between the device used for modeling and the target device affect the attack success. The effect of process variation and temperature misalignment between the profiling and target devices in the template attack's success has been studied extensively in the literature, while the impact of device aging on the template attack's success is yet to be investigated thoroughly. This article moves one step forward and studies the impact of device aging, mainly bias temperature instability (BTI) and hot carrier injection (HCI), in the devices that have been protected against power analysis attacks via dual rail logics. In particular, we focus on the wave dynamic differential logic (WDDL) circuits, and via extensive transistor-level simulations, we will show how device aging misalignments between the profiling and target devices can hinder template attacks for both unprotected and WDDL protected counterparts. We mounted several attacks on the PRESENT cipher, with and without WDDL protection, at different temperatures and aging times. Our results show that the attack is more difficult if there is an aging-duration mismatch between the training and target devices, and the attack-efficiency decrease is especially significant for mismatches of few weeks.**

***Index Terms*—Device aging, Internet of Things (IoT), side-channel attack, success rate (SR), template attack, wave dynamic differential logic (WDDL).**

Manuscript received November 1, 2020; revised April 12, 2021; accepted May 30, 2021. Date of publication June 14, 2021; date of current version April 21, 2022. This work was supported in part by the National Science Foundation CAREER Award under Grant NSF CNS-1943224; in part by the BRAINE ("Big data pRocessing and Artificial Intelligence at the Network Edge") H2020 ECSEL European Project under Grant N° 876967; in part by the French BPI through Securyzr-V Project (2021–2022). This article was recommended by Associate Editor Y. Jin. *(Corresponding author: Farzad Niknia.)*

Farzad Niknia was with the University of Maryland Baltimore County, Baltimore, MD 21250 USA. He is now with the Department of Electrical and Computer Engineering, Northeastern University, Boston, MA 02115 USA (e-mail: niknia.f@northeastern.edu).

Jean-Luc Danger and Sylvain Guilley are with the Think Ahead Business Line of Secure-IC S.A.S., Institut Polytechnique de Paris, 91764 Palaiseau, France (e-mail: jean-luc.danger@telecom-paris.fr; sylvain.guilley@secure-ic.com).

Naghmeh Karimi is with the Department of Computer Science and Electrical Engineering, University of Maryland Baltimore County, Baltimore, MD 21250 USA (e-mail: nkarimi@umbc.edu).

Digital Object Identifier 10.1109/TCAD.2021.3088803

I. Introduction

AGGRESSIVE scaling continues to push technology into smaller feature sizes and results in more complex systems in a single chip. With such scaling, various robustness concerns have come into account among which the change of circuits' specification during their lifetime, so-called device aging, has received the lion's share of attention. Due to aging, electrical behavior of transistors deviates from its original intended one, resulting in degrading the chip's performance and, ultimately, its functional failure as the chip fails to meet some of the required specifications [1], [2]. Bias temperature-instability (BTI) and hot-carrier injection (HCI) have been shown to be more prominent than the other aging mechanisms [3]–[6].

Not only does the aging degrade the integrated circuits reliability over time, but it may also affect the device from a security point of view. For example, in sensitive areas, such as wireless communication, financial systems, health care, etc., cryptographic devices are deployed to protect the data those are being analyzed and/or transferred or the tasks that are being conducted. However, these pieces of hardware, like other integrated circuits degrade over time and their degradation rate depends on their workload, operating temperature, voltage source, and the technology node. Moreover, adversaries may accelerate the aging rate via placing the target circuit under stress by feeding a specific tailored workload [7]. Although the effect of aging on the reliability of integrated circuits has been studied extensively in the literature, little research has been conducted on investigating the impact of aging on security of the devices which are supposed to be secure such as cryptographic modules.

Side-channel analysis (SCA) is an effective, cheap, and scalable technique to recover the secret keys of cryptographic chips by exploiting the physical characteristics of such devices during the process of enciphering/deciphering [8], [9]. To conduct SCA attacks, timing characteristics, power consumption, or electromagnetic emanations [10] of the target chip are measured during the enciphering or deciphering process and the gathered data are used to recover the key by investigating the correlation between these measurements and the secret data.

Differential power analysis (DPA) [11], correlation power analysis (CPA) [12], mutual information analysis (MIA) [13], and template attacks [14] are among the attacks that grabbed a lot of attention in the recent years. The first three are categorized as nonprofiling attacks, i.e., they do not need a golden chip to characterize a target chip and retrieve its key. However, the template attacks, the most common form of profiling attacks, rely on a golden model based on which a template is built and used to attack a chip with a similar implementation. Template attacks are known to be the most powerful attack from an information theoretic point of view as they maximize the success probability [15]. Such attacks are naturally *multivariate*, i.e., they can exploit simultaneously several leakage samples.

Due to the strength of template attacks, in this article, we focus on such attacks and their effectiveness in the presence of aging, temperature, and process variation mismatches between the device used to built the template and the target device. Actually, we analyze how the quality and success rate (SR) of the template attack is affected by deviations resulted from the aforementioned mismatches. In practice, the measured characteristics of a golden (profiling) chip may not match the target device specially in case of aging.

Although we can prevent temperature mismatch by controlling the measurement temperature for both profiling and target devices, it may not be possible to align the age of both devices. Such aging-induced deviations can affect the SR of the template attack [16]. On the other hand, to protect the cryptographic chips against power analysis attacks, different countermeasures have been proposed in the literature to cover the dependency between the power consumption and the data being process. Dual rail logics [17] are widely used for such purposes. However, the balancing provided by these logics may be voided when device aging comes into account as each of the dual paths may age differently considering the different type of gates each includes. Accordingly, there is a need to thoroughly investigate the impact of aging on the template attacks launched on dual-rail logic frameworks. This article targets one common type of dual-rail logics, the so-called wave-dynamic differential logic (WDDL), which is discussed in more detail in Section II-C, for such analysis. The contributions of this article include as follows.

1) A simulation framework that integrates device aging and its security evaluation against template attacks.
2) Detailed HSpice MOSRA simulations to evaluate the effect of BTI and HCI degradations on the SR of template attacks launched on the PRESENT cipher (S-box).
3) Extracting perceived information (PI) to assess the level of security against attacks launched on aged devices.
4) Investigating the impact of aging mismatches on the success of the template attacks launched on WDDL-protected devices.

The remainder of this article is organized as follows. Section II presents the preliminary backgrounds required for this study. Section III discusses the threat model. Section IV discusses the motivation of this research and argues how the template attack is affected by various mismatch of training and attack devices. Section V presents the experimental setup followed by the experimental results in Section VI. Section VII discusses our findings and observations. Finally, Section VIII concludes this article and draws the future extensions of this research.

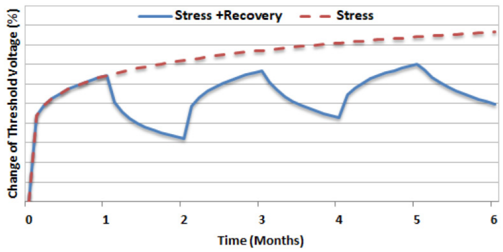


Fig. 1. Threshold-voltage shift of a pMOS transistor under NBTI effect.[1]

II. Preliminaries

A. Background on Aging Mechanisms

Aging mechanisms, including negative-BTI (NBTI), positive-BTI (PBTI), HCI, time-dependent dielectric breakdown (TDDB), and electro-migration (EM) result in performance degradation and eventual failure of digital circuits over time [18]. In practice, NBTI, PBTI, HCI, and TDDB all affect the gate oxides of transistors while EM occurs in the interconnect metal lines. Among the aging mechanisms, BTI (including both NBTI and PBTI) and HCI are two leading factors in performance degradation of digital circuits [19]. Both mechanisms result in increasing switching and path delays in the circuit under stress [20]. This will eventually lead to timing violations and finally faster wear out of the system. Thereby, both mechanisms jeopardize the reliability of digital circuits. NBTI mainly affects pMOS transistors, while PBTI and HCI targets nMOS transistors.

BTI Aging: A pMOS transistor experiences two phases of NBTI depending on its operating condition. The first phase, the so-called stress phase, occurs when the transistor is on ($V_{gs} < V_t$). In this case, positive interface traps are generated at the Si-SiO$_2$ interface which lead to an increase of the threshold voltage of the transistor. The second phase, the so-called recovery phase, occurs when the transistor is off ($V_{gs} > V_t$). The threshold voltage drift that occurred during the stress phase will partially recover in the recovery phase.

Threshold voltage drifts of a pMOS transistor under stress depend on the physical parameters of the transistor, supply voltage, temperature, and stress time [2]. The last three parameters (the so-called external parameters) are used as acceleration factors of the aging process. Fig. 1 shows the threshold voltage drift of a pMOS transistor that is continuously under stress for six months and a transistor that alternates stress/recovery phases every other month. As shown, the NBTI effect is high in the first couple of months but the threshold voltage tends to saturate for long stress times.

It is noteworthy to mention that PBTI affects nMOS transistors in a similar way that NBTI affects pMOS transistors. Indeed, the impact of NBTI is more dominant than PBTI beyond the 45-nm technology node. However, with the introduction of high-k gate dielectrics and metal gate transistors, PBTI effects have also received significant attention [21].

HCI Aging: HCI occurs when hot carriers are injected into the gate dielectric during transistor switching and remain there.

[1] Values on the y axis are not shown to make the graph generic for different technologies.

HCI is a function of switching activity and degrades the circuit by shifting the threshold voltage and the drain current of transistors under stress. HCI mainly affects nMOS transistors.

HCI-induced threshold voltage drift is highly sensitive to the number of transitions occurring in the gate input of the transistor under stress. In practice, HCI has a sublinear dependency on the clock frequency, usage time, and activity factor of the transistor under stress, where the activity factor represents the ratio of the cycles the transistor is switching and the total number of cycles the device is utilized. HCI effects depend on the operating temperature [19].

In this research, to evaluate the impact of NBTI, PBTI, and HCI on the current (and, in turn, on the power signature) of a device under stress, HSpice MOSRA (MOS Reliability Analysis) [22] is deployed. MOSRA uses the Reaction-Diffusion (R-D) model discussed in [23].

B. Background on PRESENT Cipher

PRESENT is an international standardized (ISO/IEC 29192-2:2019) lightweight block cipher with 64-bit blocks and a bit oriented permutation layer [24]. It includes 31 rounds and supports two key lengths of 80 and 128 bits. Each encryption round consists of a bitwise XOR operation, a nonlinear substitution layer and a linear permutation layer. The nonlinear layer uses a single 4-bit S-box which is applied 16 times in parallel in each round [25]. In this article, we mainly concentrate on the S-box, since it is the most interesting target for attackers (owing to its contrasted confusion coefficient [26]).

Note that PRESENT has been chosen for its popularity as a representative block cipher in the embedded systems security [27], [28]. The advantage of PRESENT S-box is that it is small enough to be executed in one clock cycle, even after protection [refer to the shallow netlist of Fig. 3(b)]. In contrast, AES S-box has a lot of different implementations (fast / compact / etc.), and its implementation with protection usually requires a breakdown in smaller parts [29], typically considering it with nibble-oriented datapath (as is the case of PRESENT).

C. Background on WDDL

WDDL [30] is a gate-level logic style, which smooths side-channel fluctuations induced by sensitive data, and has the advantage of being systematic (automatable whatever the initial design) and standard-cell based. WDDL results from a series of transformations which can be automated from a regular (so-called: single-ended) netlist. These transformations aim at ensuring two properties.

1) Turning computation into two phases, namely, *evaluation* and *precharge*, such that all nets have no or only rising edge in evaluation, and those nets which had a rising edge in evaluation have a falling edge in precharge.
2) Each bit is split in two bits, termed *true* and *false*, whose activity is complemented: when the true bit toggles, the false bit remains quiet, and vice-versa.

Therefore, a WDDL netlist has $2N$ gates (as many true as false gates), from which N gates featuring a raising edge in evaluation, and similarly N gates (the same gates) featuring a falling edge in precharge. This results that the following.

1) Assuming the leakage model is Hamming weight, the leakage is constant, equal to N.
2) Assuming the leakage model is Hamming distance, the leakage is constant, also equal to N (assuming the circuit is initialized with all the gates at 0 state).

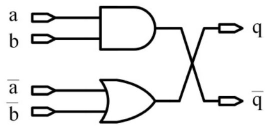


Fig. 2. WDDL AND/NAND gates.

There are multiple ways to transform a single-ended netlist into a WDDL netlist. We provide here one example.

1) The synthesis is constrained to use only monotonous gates, i.e., gates whose output increases or decreases when inputs increase. Example of such gates are AND/OR (positive gates) or NAND/NOR and INV (negative gates). Notice that all monotonous gates are either positive gates or negative gates followed by an INV. Also remark that any function can be expressed by the composition of positive and negative gates, since the set (AND, INV) is universal.
2) This single-ended netlist is turned in WDDL logic by the application of gadgets. Flip-flops are turned into a pair of flip-flops, each being asynchronously initialized at zero, and reset synchronously upon precharge phase. Positive gates f are replaced to a pair $(f, \tilde{f})$, where $\tilde{f}$ is the dual of f with respect to complementation, in that $\tilde{f}(x) = \neg f(\neg x)$. Notice that $\tilde{f}$ is positive if f is. Decreasing gates are decomposed into a positive gate and an INV. INV gates are replaced by a wire crossing between true and false inputs.
3) Eventually, inputs are turned into WDDL protocol, in that they alternate $(0, 0) \to \{(0, 1), (1, 0)\} \to (0, 0) \to \cdots$ Likewise, outputs consist in selecting the true value (while dropping the false one), and ignoring values upon precharge.

The WDDL logic is endowed with a very simple leakage model, which is basically constant, i.e., irrespective of manipulated data. At least, this holds for a leakage model which consists in the count of set bits (in the Hamming weight model) or the total toggle count (in the Hamming distance model). When looking at a finer scale, it happens that combinational gates can have so-called “shortcut evaluations,” in that an OR gate evaluates true as soon as one input is set, irrespective of the second one. Now, the dual of OR is AND (since $\widetilde{\mathrm{OR}}(a, b) = \neg(\neg a \vee \neg b) = a \wedge b = \mathrm{AND}(a, b)$), which can evaluate early in precharge (in that $\mathrm{AND}(1, b)$ depends on b, namely, it is equal to b). Fig. 2 shows an AND/NAND gate implemented in WDDL format. In precharge phase, $a = b = \bar{a} = \bar{b} = 0$, which results in $q = \bar{q} = 0$ as well (wave propagation). In evaluation phase, $\bar{a} = \neg a$ and $\bar{b} = \neg b$, which results in $\bar{q} = \neg q$ as well (duality condition).

To solve the early propagation effects [31], improvements of WDDL have been suggested, yet they are making the design much more complex and the design flow much less automatable. Thus, we do not consider them in this article, and instead live with the shortcomings of WDDL. We will explain in which respect WDDL is an acceptable countermeasure, in terms of security versus performance overhead ratio. In particular, WDDL has been highly optimized [32], and also features remarkable resilience to fault injection attacks [33].

Indeed, dual-rail logics have been first introduced in 2003 [17] to mitigate power analysis attacks. To compromise this countermeasure, some attacks were introduced in literature that consisted in model-based power analysis, e.g., [34], [35], to exploit differences in placement. Tools soon shifted from regular attacks to leakage estimation tools, such as (MIA [13]). For example, [13] shows that Dual Rail Precharge Logic is best analyzed with MIA. Now, MIA is basically a nonprofiled information-theoretic distinguisher, whose supervised equivalent is the so-called "template attack" [14] on which we focus in this article.[2]

D. Background on Template Attacks

Side-channel attacks represent one of the most powerful category of attacks launched by adversaries to obtain secret information of a device, e.g., a cryptographic key. These attacks retrieve the secret key by analyzing the physical leakage emitted during operation of a device (e.g., its running time [37], power consumption [37], and electromagnetic radiation [38]), as this leakage is statistically dependent on the secret key. Profiled side-channel attacks are the most powerful type of side-channel attacks in which an attacker is able to characterize the leakage of an additional similar device and use the extracted information to break the targeted device.

Template attacks are one of the most commonly used profiling attacks and known to be the most powerful attacks from an information theoretic point of view [14]. These attacks are launched in two phases: 1) training and 2) attack. In the training phase, the attacker has a full control on another copy of the protected device. He/She records a large number of traces of the cloned device, corresponding to random values of inputs (plaintexts and keys). These traces are utilized to build a template y_k from the device, using key k. Then, in the attack phase, the recorded traces are classified according to the value of the key and template matching is performed to derive the key value of the device under attack [14]. In particular, if traces are represented as a matrix X of $D \times Q$ real numbers (Q traces of $D = 300$ samples as an example), and the learned model Y_k is also a $D \times Q$ matrix, then the attack guesses the key as [39, Th. 1]

$$\hat{k} = \underset{k \in \{0,1\}^4}{\operatorname{argmin}} \operatorname{tr}\Big((X - Y_k)^{\mathsf{T}} \Sigma^{-1} (X - Y_k)\Big) \tag{1}$$

where Σ is the $D \times D$ noise covariance matrix, tr is the trace operator, and argmin operator selects the value of k (4 bit value) that results in the minimum value of its following function.

In this article, we aim at studying template attacks in terms of SR, by analyzing how factors such as aging, temperature and process variation affect them. We investigate these effects on both unprotected PRESENT cipher as well it WDDL-protected counterpart. We consider an ideal setup (for the attacker) where training and attacked devices are otherwise equal, but different in terms of aging, process variations, and temperature. In practice, the actual discrepancy results from a combination of those three (or even more) mismatch factors. We will quantify how these factors contribute in decreasing the SR of template attacks for the unprotected and the WDDL-protected ciphers.

III. Threat Model

WDDL has been designed to make "*a priori* model" power attacks impossible as in a WDDL-protected circuit, it is expected that the leakage from the states has its power balanced. Thereby, no model can be devised to leak the secret data. This is the theoretical rationale. However, in practice, the exact balancing of gates leakage is limited to the extent that the dual gates are otherwise equal, and likewise routed alike, since leakage results both from the gates activity and the resulting signal propagation in the interconnect. Although the balancing is close to perfect, signal acquisition techniques can be geometrically accurate enough to capture one wire in a pair more precisely than the other, thereby unbalancing them through the accuracy of the measurement setup. Considering the high integrity of digital circuits, the difference of size between the user's logic and attacker's probe is quantitative (several orders of magnitude in the current state-of-the-art). This make such unbalancing difficult, if not impossible. On the other hand, the combinational logic can have leakage as well, yet exploitation of combinational logic is more difficult since it does not occur at the same point in time. Therefore, only machine-learning-based attacks (that is, template attacks) are realistic for WDDL-protected circuitries.[3] To be successful, such attack should be able to control the target cryptographic engine, e.g., by selecting inputs.

Note that in most cryptographic circuits, the key cannot be chosen by the user (it is either produced by a PUF, or arises from a key management system, etc., and in any case is protected against corruption). Thereby, the time it takes for the attacker to work around all those difficulties and collect "training" traces to launch machine-learning-based attacks, such as template attacks, is nonnegligible and such effort can results in a large a discrepancy between the aging of the target and the chip used for modeling. Accordingly, in this article, we take such aging misalignment into account and investigate how such aging discrepancy between the template and the target device affects the attack outcome.

Eventually, we consider in our threat model that the user can be malicious, and therefore attempt to degrade the countermeasure by submitting the device to stress, such as abnormally high temperature [40]. Indeed, operating the chip beyond nominal temperature can result in imbalances in the dual-rail

[2] It is proven in this paper [36] that the Maximum Likelihood distinguisher (i.e., template attack) is equivalent to MIA, when leakage probabilities are replaced by online estimated probabilities.

[3] Attacks resorting to *a priori* models, such as CPA, indeed cannot apply reliably because the leakage model is unknown.

protected system and can facilitate side-channel nonprofiling attacks. Accordingly, we consider in the sequel a broad range of temperatures, from −40 to 125 °C.

IV. Aging-Related Mismatch Between Template and Attack Data

Side channel attacks focus on creating a proper key-dependent leakage model that when compared with actual measurements can recover the key. The more accurate the model, the higher the success of the launched attack [41]. Even though profiling attacks, e.g., template attacks, include an offline learning phase to estimate the leakage model, the profiling method is based on some assumptions (such as Gaussian noise models) or even model estimation that can be bounded by the number of measurements during the characterization. Thereby, one of the main challenges in these attacks is to avoid being biased by an incorrect model [41].

As mentioned earlier, it may not be possible to provide the same operation conditions during both profiling and matching phases, i.e., operating temperature, process variation, and aging effects can be different. The problem can be exacerbated when power-equalized cryptographic circuits are targeted. The dual-rail logics and in particular WDDL may intensify the discrepancies occur regarding the aforementioned mismatches as each of the rails may be affected differently from the other one.

In this article, we mainly focus on the unavoidable aging deviations and investigate their effects on the WDDL protected logics. The impact of process variation and temperature misalignments between the profiling and targeted devices will be also discussed to show how each of these mismatches contribute in changing the SR of the template attack when a WDDL protected device is targeted compared to when an unprotected device is compromised. In practice, it is difficult (if not impossible) to align the age of the profiling and the target devices. One option could be to "accelerate aging" in the newer device (whether it is the profiling component or the target one) by artificial aging (e.g., placing the chip in a dedicated climate chamber to accelerate aging). However, as aging degradation rate changes exponentially with the drift of operating conditions [42], a slight deviation in the input parameters strongly impacts the acceleration rate. Thereby, it is interesting to quantify how much the security is impacted by the unavoidable effect of aging.

Indeed, both combinational and sequential logics are faced with the problem of information leakage in power analysis attacks. However, as the leakage amount is more considerable in combinational gates, these gates are mainly targeted in side-channel attacks. Thereby, in this article, we target the S-box module of the PRESENT cipher.

V. Experimental Setup

In this article, we implemented the add-round-key and S-box operations in the first round of the PRESENT cipher with 80-bit keys in the transistor level once with ordinary gates and later by applying the WDDL technique using a 45-nm technology extracted from the opensource NANGATE library [43]. Our implementation represents the most compact S-box architecture presented in [44]. Though the gate-level netlist [Fig. 3(a)] is the most minimal size, it includes a long critical path with several XOR gates, which makes it highly amenable to glitches that complexify the link between input data and leakage. In addition, the equivalent WDDL protected circuit has been depicted in Fig. 3(b). Thereby, according to the aforementioned explanation about the characteristics of this design, the circuit is highly suitable as a case study for Template attacks (which have a strong advantage if the model is accurately profiled).

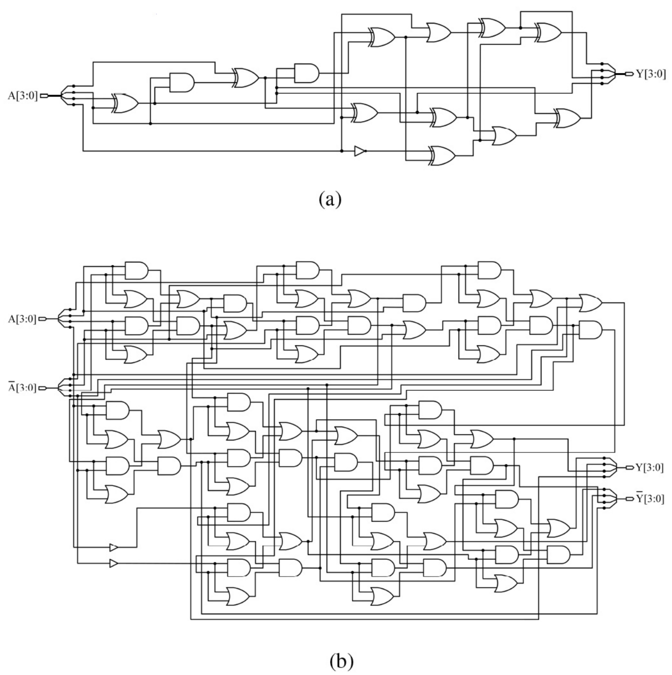
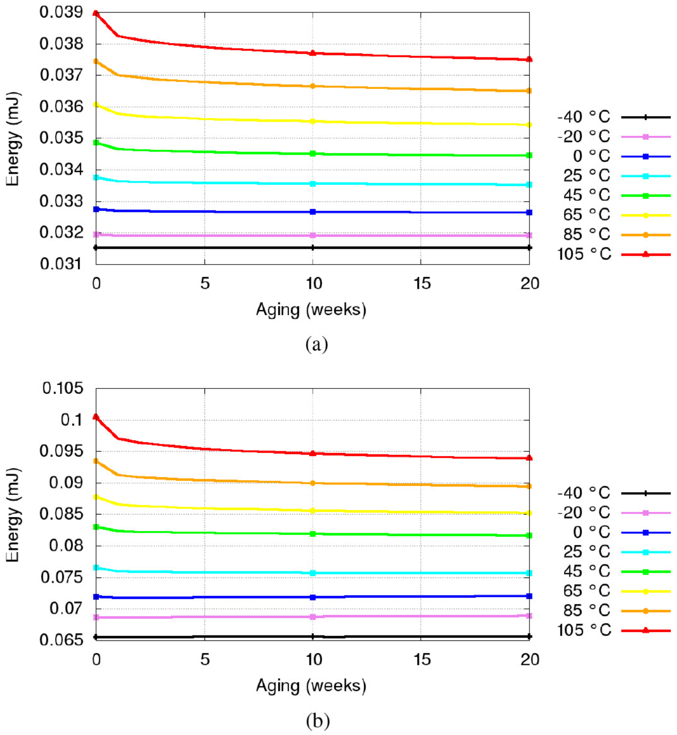


Fig. 3. Netlist of the PRESENT S-box considered in this study. (a) Unprotected S-box. (b) WDDL-protected S-box.

We used Synopsys HSpice for the transistor-level simulations and deployed the HSpice built-in MOSRA Level 3 model to assess the effect of NBTI, PBTI, and HCI aging [22]. For both unprotected and WDDL-protected circuitries, power traces were extracted for a fresh (nonaged) device as well as aged devices. The effect of aging was evaluated for 20 weeks of device operation in time steps of one week. The experiments were conducted assuming different operating temperatures including {−40, −20, 0, 25, 45, 65, 85, 105 °C}.

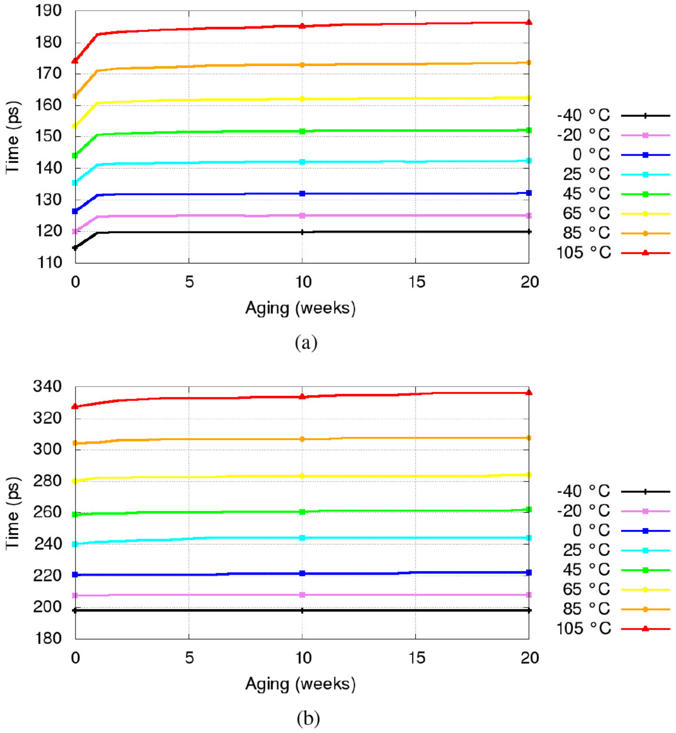
For the WDDL-protected circuit, as each S-box module in the PRESENT cipher has $n = 4$ input bits, we have a total of $2^n = 16$ input transitions in the S-box. Recall that all signals get the value of "0" in the precharge phase. Cryptographic functions, by essence, randomize the data they manipulate. Therefore, it is natural that in "steady cruising speed," all possible transitions are considered with an equal probability of 2^{-n} (here, $1/16$ when $n = 4$) for the WDDL-protected circuitry. The actual order of the transitions has no real impact as long as all transitions are asymptotically equiprobable. On the other hand, for the unprotected device, we have a total of $2^{2n} = 256$ input transitions in the S-box. To have a fair



(a)

(b)

Fig. 4. Average energy consumption in S-box for different temperatures and aging durations. (a) Unprotected S-box. (b) WDDL-protected S-box.



(a)

(b)

Fig. 5. Average propagation delay of S-box for different temperatures and aging. (a) Unprotected S-box. (b) WDDL-protected S-box.

comparison between the unprotected and WDDL-protected circuitries, 16 transitions were considered in the profiling phase of the template attacks for each of these circuitries. The simulated traces contain two parts: 1) the results of key addition and 2) S-box outputs for each initial n-bit value as well as its following n-bit value. For the attack, we considered only the second clock cycle, when the cryptographic circuit transitions from *initial* to *final* value. Fig. 13 shows sample waveforms.

VI. Experimental Results

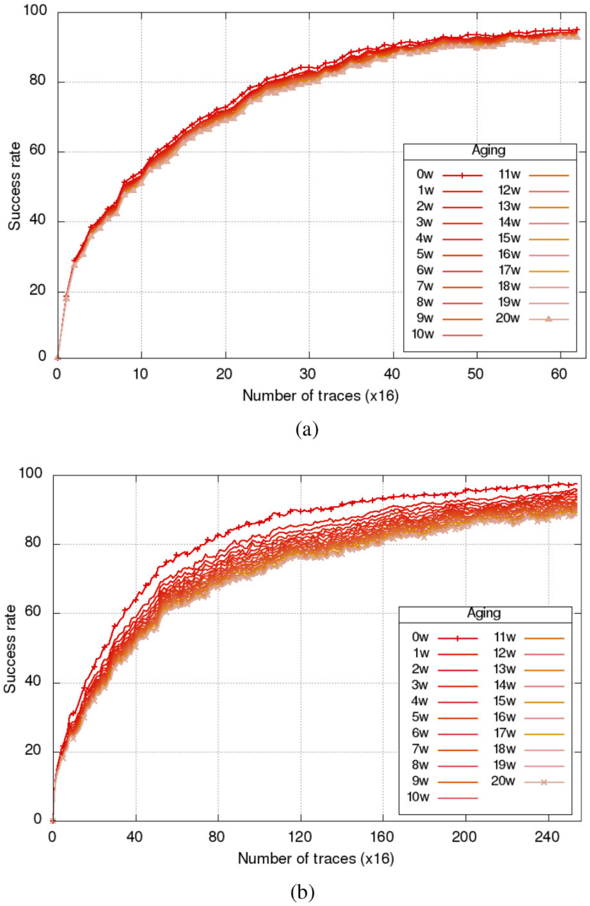
A. Impact of Aging on Average Energy Consumption in S-Box

The first set of results deals with the effect of aging on the energy consumed to compute S-box outputs in each of unprotected and WDDL-protected circuitries. To compute the average energy consumption of S-box, we first performed extensive HSpice simulations for S-box circuits in each case using all 256 input transitions for the unprotected circuits and all 16 transitions in the WDDL-protected counterpart. Then, we recorded the instantaneous power consumption related to each input transition over time. We repeated the simulations for different temperatures and different aging times. Then, we evaluated the average energy consumption of S-box using the recorded values. Fig. 4(a) and (b) illustrates the average energy consumption for the unprotected and WDDL circuits, respectively. As expected, the average energy consumption decreases over time. This is because aging results in the increase of the threshold voltage of transistors under stress and accordingly in the decrease of the drain current through them. The aging-related degradation is more visible in the first few weeks of device operation. Moreover the increase of temperature results in more energy consumption in both circuits.

Although the power consumption in the WDDL circuitry follows the same pattern as the unprotected one, its magnitude increased approximately 2–2.5 times since WDDL includes around 2× gates compared to the unprotected circuits. The take-away point of this observation is that due to the aging the power traces change over time and, accordingly, profiling attacks such as template attacks need to consider aging effects while profiling/matching is conducted.

B. Impact of Aging on the Average Propagation Delay of S-Box

The second set of results investigates the effect of aging on the propagation delay of the S-box. We extracted the propagation delay related to each trace (i.e., each input transition) separately for both unprotected and WDDL-protected circuits and computed the average delay for each temperature and aging duration. To evaluate the delay of the S-box for each input transition, we extract the time needed to propagate each transition from the input to the output of the S-box. Fig. 5(a) shows the propagation delays for the unprotected S-box and Fig. 5(b) depicts the delay values for the WDDL counterpart. As expected, in both circuits, the propagation delay increases over time. That is because aging degrades the performance of the device under stress. Moreover, performance degradation is worse in higher temperatures as the BTI aging rate increases exponentially with the temperature increase. The degradation is higher in the first weeks of aging. The take-away point from



(a)

(b)

Fig. 6. SR after 1000 attacks for different ages of the target device. Profiling Temperature = 105 °C, Attack Temperature = 105 °C, and $\sigma = 0.032$. Profiling device is new. (a) Unprotected S-box. (b) WDDL-protected S-box.

this observation is as aging changes the time needed to provide each output value, the profiling attack can become more difficult if the profiling and template devices have been aged differently.

C. Impact of Aging on the Attack Success Rate

This set of results investigates the effect of aging on the SR of the template attack. In this experiment, profiling and attack temperatures were equal. However, the training traces were gathered from a fresh device (i.e., 0 week aging shown as 0w in Fig. 6(a) and (b) for the unprotected and WDDL-protected circuits, respectively), while attack was mounted on a device aged in the range of 0 and 20 weeks (shown as 0w to 20w in the figure). As our HSpice simulations with MOSRA do not consider noise, to realize the experiments, we added some level of white noise in our analysis.

Remark 1 (On Signal-to-Noise Ratio): Noise arises from multiple sources, mostly independent from the design under analysis, and shall be considered in the end-to-end side-channel analysis setup, which can be viewed as a digital communication problem [45]. One can partition noise according to its origin as follows.

1) Some noise is termed "algorithmic" as it is incurred by the surrounding logic which performs unrelated computations.
2) Some noise is intrinsic to the "measurement" since it comes from the noise figures of the measurement setup. This is modeled in Annex B of ISO 20085-1:2019.

All those sources add up and can be modeled by an AWGN (Gaussian noise).

Fig. 6(a) and (b) shows the SR of attacks when the temperature is 105 °C and $\sigma = 0.032$, where σ denotes the standard deviation of the noise considered in our analysis. Note that we considered a large amount of noise ($\sigma = 0.032$), compared to the signals (with standard deviation $\approx 150\ \mu$W in the unprotected circuit), resulting in signal-to-noise ratio of ≈ 0.005 (typical value, see [46, Fig. 8, Appendix A]). As shown for both unprotected and WDDL circuits, the SR decays with aging, as the attacked circuit becomes older and older with respect to the clone used to build the templates. The SR drops fast after one week, and then continues to decrease, albeit at a slower rate.

As depicted in Fig. 6, at 105 °C, the number of traces to reach 80% SR when the target device is new is approximately three times more for the WDDL circuit compared to the unprotected counterpart (26×16 for unprotected compared to 73×16 traces for WDDL). This ratio is around 5× for a 20-week-old target device (32×16 compared to 155×16 traces for unprotected and WDDL circuits, respectively). Such aggressive increase of the required traces for WDDL compared to the unprotected circuit is due to the imbalances occur due to the aging in the dual rails which act similar to a measurement noise resulting in dropping SR, and the need of more traces for a successful attack.

The law (2) can be interpreted as follows: to increase the SR of an attack from 90 number of traces is needed. Fig. 5(b) shows the result of fitting to (2), using linear regression.

The value of the SR seems noisy in Fig. 6(a) and (b). This is due to the fact that simulating SRs are prone to estimation errors (though we resorted to 1000 attacks). One common practice in the side-channel analysis is to *smooth* the SR curve. However, for more sensible approximation, we consider that empirical SRs (Fig. 6) can be fitted by the exponential law shown in (2), where q is the number of traces and the constant e is the *first-order SR exponent* [47] whose theoretical value can be expressed as a linear function of the signal-to-noise ratio and algorithmic confusion coefficient [48]. In practice, the value of $e \in \mathbb{R}^+$ is extracted by fitting (2) to the experimental data

$$\mathsf{SR} = 1 - \exp(-e \times q). \tag{2}$$

The law (2) can be interpreted as follows: to increase the SR of an attack from 90% to 99% (resp. from 99.0% to 99.9%), twice number of traces is needed. Fig. 7(a) and (b) shows the fitted form of Fig. 6(a) and (b) using 2, zoomed around 80% of SR.

To investigate the effect of temperature, Fig. 8(a) and (b) compares the number of traces needed to reach the SR of 80% for the attacks launched at 65 °C and 105 °C. In both temperatures the number of traces to attain 80% success is increasing fast in the first week of aging, and then it grows with a slower rate. This increase of the number of required traces is more prominent in WDDL circuits compared to the unprotected one.

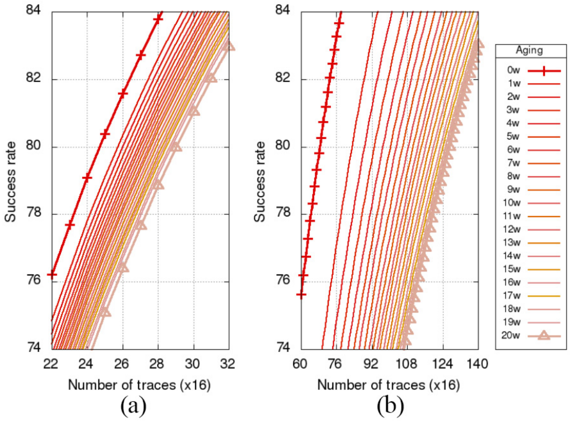


Fig. 7. Zoom on the fitted result of window around SR = 80 displayed in Fig. 6(a) and (b) using (2). (a) Unprotected S-box. (b) WDDL protected S-box.

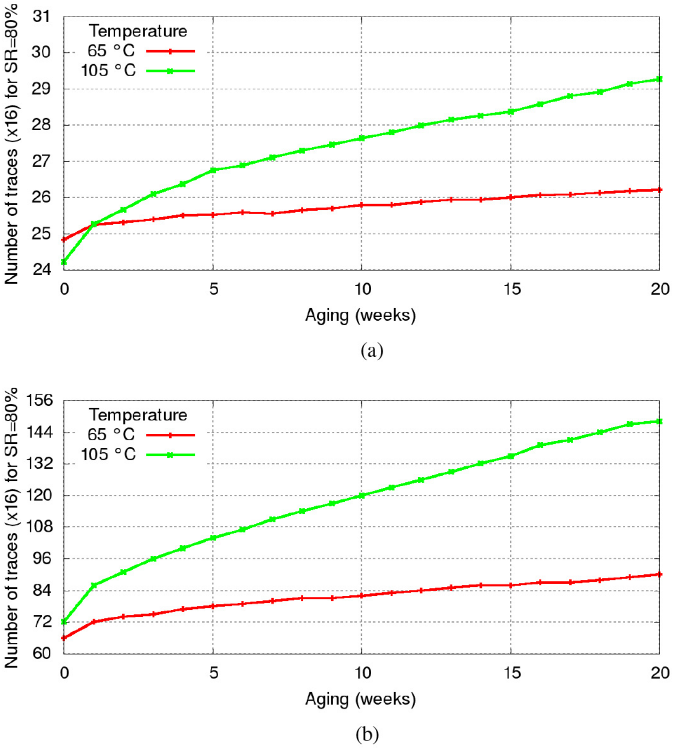


Fig. 8. Mean number of traces to reach SR = 80% (σ = 0.032) when the target device has different ages. In each case profiling and attack temperatures are equal, and the profiling device is new. (a) Unprotected S-box. (b) WDDL-protected S-box.

In particular, at 105 °C, to attain the 80% SR, a five-week old WDDL circuit requires 44.4% more traces compared to its new counterpart but the five-week old unprotected circuitry needs 10.4% more traces compared to a new unprotected circuit. The rate increases to 105.5% and 20.8% for the WDDL and unprotected circuits, respectively, after 20 months of aging at 105 °C.

Another interesting observation made Fig. 8(a) and (b) is that temperature increase makes the attack more difficult. i.e., more traces are needed for a successful attack in higher temperature for both protected and unprotected circuits. For example, the number of traces required to break the key in the WDDL circuit with a probability of 80% at 105 °C will increase ≈ 105.5% in the course of 20 week of usage while increases 36.3% when the temperature is 65 °C. Note that in each case, the number of required traces is 16 times of the *y*-ordinate. To highlight the effect of aging and avoid mismatches caused by process variation, in this figure, we do not consider process variation.

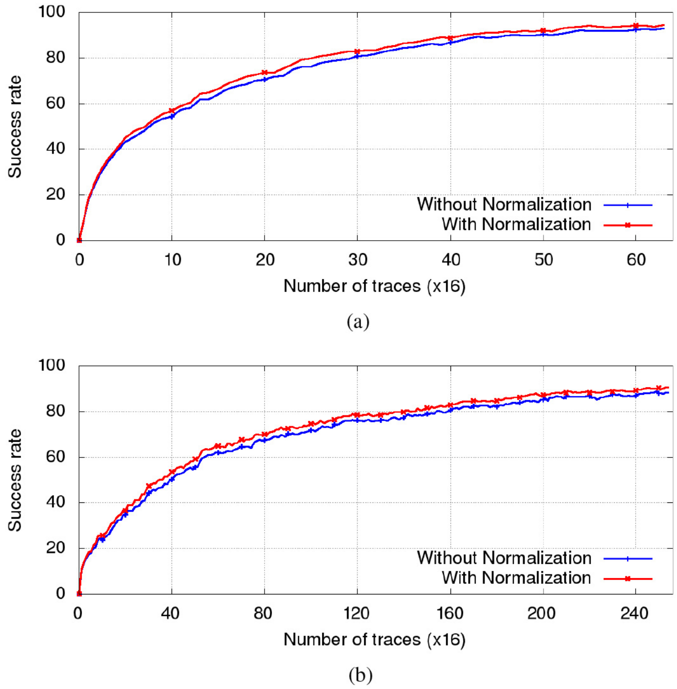


Fig. 9. SR after 1000 attacks with and without applying normalization [49] on a 20-week old unprotected and a 20-week old WDDL-protected target circuits. Profiling Temperature = 105 °C, Attack Temperature = 105 °C, and σ = 0.032. Profiling device is new. (a) Unprotected S-box. (b) WDDL-protected S-box.

To mitigate deviations between profiling and matching phases, template normalization has been proposed in [49] where both 2^n templates $\hat{p}$ (for all the values of the key) and 2^n online distributions $\tilde{p}$ are transformed by homothety such that they have the same *zero mean* and *unit variance*. The next set of results shows how normalization affects the success of template attack when there is an aging mismatch between profiling and matching devices. In Fig. 9(a) and (b) the template device is new while the target device is 20-week old. As shown, normalization slightly helps to improve the attack via reducing the number of traces, but does not impact our conclusions. In particular, via normalization, the number of traces required to break the key of an unprotected circuit with a probability of 80% decreases ≈16% when there is a 20-week aging mismatch and temperature is 105 °C. Such decrease is around 10% for a WDDL-protected circuit.

D. Impact of Process Mismatch

Considering the imperfections of the manufacturing process, in practice, the devices used for training and matching phases behave slightly different even if we ignore the aging

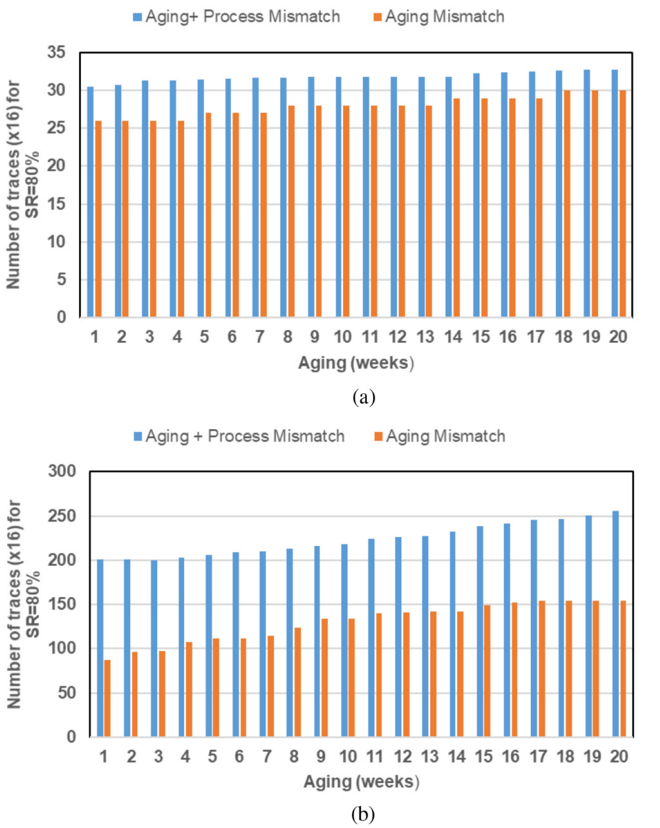


Fig. 10. Mean number of traces to reach SR = 80% with and without process variations. Profiling Temperature = 105 °C, Attack Temperature = 105 °C, and $\sigma = 0.032$. (a) Unprotected S-box. (b) WDDL-protected S-box.

and temperature mismatches, i.e., there is a process-variation-induced mismatch between these devices. Accordingly, process variations need to be taken into account while assessing the attack success. Fig. 10(a) and (b) compares the number of traces required to attain 80% success when both aging and process variations are considered with the case when only aging is considered. Simulations were carried out using a Gaussian distribution: transistor gate length $L : 3\sigma = 10\%$; threshold voltage $V_{TH} : 3\sigma = 30\%$, and gate-oxide thickness $t_{OX} : 3\sigma = 3\%$.

In these experiments, we used the Monte Carlo simulations to model 30 chips (C_i where $1 \leq i \leq 30$) in order to investigate the effect of process variation on the attack SR. In these experiments, the template was built based on the power traces extracted from C_1 at 105 °C when it was new (i.e., age = 0). Then for each chip, the number of traces required to attain the SR of 80% was calculated for different ages of the target device. The bars shown in blue in Fig. 10(a) and (b) show the average number of traces required to reach SR = 80% when the unprotected chips and WDDL-protected counterparts were targeted, respectively. We repeated the experiments when for each aged targeted chip, we built the template using the power traces of the same chip when it was new (age = 0), thus ignored the effect of process variations. These experimented were conducted at 105 °C. The bars shown in red in Fig. 10(a) and (b) represent the average required traces to reach SR = 80% when these attacks are launched on the unprotected and WDDL-protected circuits, respectively.

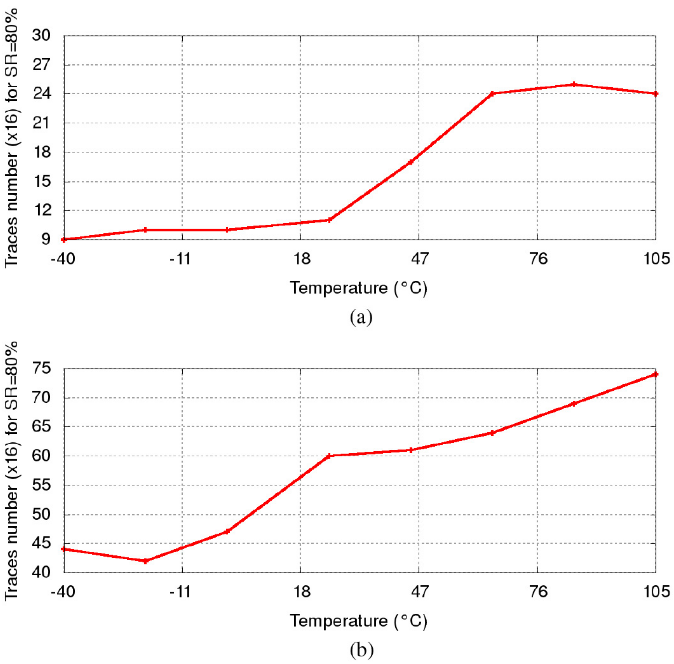


Fig. 11. Mean number of traces to reach SR = 80% when template and attack temperatures are the same. Both template and target devices are new. (a) Unprotected S-box. (b) WDDL protected S-box.

The first takeaway points from these observations is that as expected the process mismatch hinders the template attack. For the unprotected circuitry the process plus aging mismatch results in 14.5% and 10.6% increase of the number of traces after 10 and 20 weeks on top of the aging mismatch increase of 7.7% and 15.3% to attain 80% success (compared to the case of 1-week old device). For the WDDL S-box, due to the process variations the number of traces to attain 80% accuracy increases 63% after ten weeks and 66% after 20 weeks of aging. The second takeaway points from these observations is that process variations effects on WDDL circuitries is higher than unprotected circuits considering the imbalances that such variations create in the dual rail logics.

E. Impact of Temperature Mismatch

This set of results depicts the impact of temperature on the template attacks. We first show the required number of traces to reach $SR = 80\%$ when the template and target devices operate in the same temperature. Fig. 11 illustrates the results. As shown the number of traces in each temperature varies in range of 9x16 to 25x16 for unprotected circuit. This range is 42x16 to 75x16 for the protected device. The higher the temperature the more difficult the attack. A small fluctuations in results relates to the randomness of the measurement noise added artificially to the extracted simulated data.

The next set of results depicts the effect of temperature mismatch. In these experiments, profiling was conducted in 0 °C while attack was performed in different temperatures. Both profiling and attack were conducted on a new device. The results are shown in Fig. 12(a) and (b) for unprotected and protected circuits. As expected, the attack is more difficult when there is a mismatch in profiling and attack temperatures.

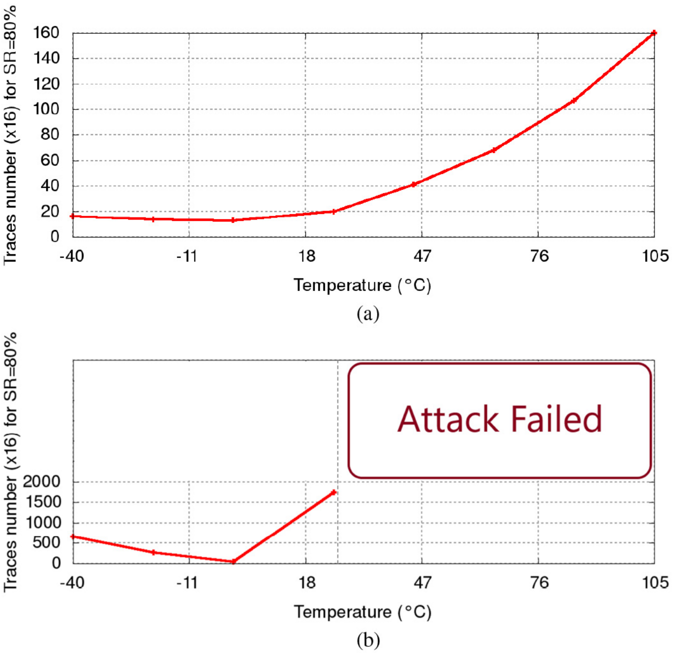


Fig. 12. Mean number of traces to reach SR = 80% when template and attack temperatures are different. The template temperature = 0 °C and the attack temperature varies between −40 °C and 105 °C. Both template and target devices are new. (a) unprotected S-box. (b) WDDL protected S-box.

For the unprotected circuit, the number of traces for attacks in −40 °C, −20 °C, and 0 °C are approximately similar; however, we can see that the global minimum value located at temperature 0 °C, as it is the temperature at which our models were built in this set of experiments. The results confirm that the attack is more difficult when there is a temperature mismatch between profiling and attack process. The impact of temperature is to increase the number of traces required to attain 80% success by ≈ 900%, considering the corners −40 °C & +105 °C for the unprotected design. For the WDDL circuit, the increase in number of traces will be significant as well and in higher temperatures the attack was somehow unsuccessful [where the number of traces is shown as infinity in Fig. 12(b)]. Indeed, the difficulty of the attack (in terms of number of traces) will be exacerbated when both temperature and aging time are not aligned between the profiling and target device. The take away point from these observations is that to decrease the number of traces required for the template attack, first, the temperature must be the same for the training and matching devices. Then, ideally, aging should be balanced. However, the latter is not always possible as activity of trainee and attacker are not similar.

F. Perceived Information Metric

Template attacks are known to be optimal (as they maximize the key recovery SR) if the profiling is perfect. In this case, an attacker can measure the mutual information (MI) [50] between the secret variable (called here $K \in \{0,1\}^n$) and the multivariate measurements (called here $\mathbf{X} \in \mathbb{R}^D$, where D is the number of samples in the traces):

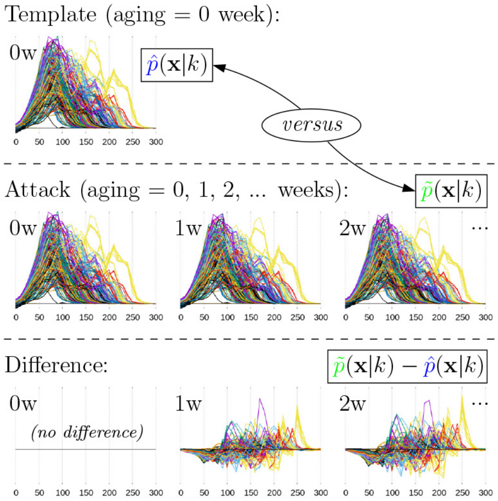


Fig. 13. Distributions for templates ($\hat{p}$) *versus* for matching ($\tilde{p}$), which are aged longer, without noise ($\sigma = 0$) for the unprotected circuit. The differences of distribution $\tilde{p}$ and $\hat{p}$ is also represented. Abscissa represents samples $(0, \ldots, D-1)$ and colors the different $k \in \{0,1\}^4$.

$$\mathsf{MI}(\mathbf{X}, K) = \int_{\mathbf{x}\in\mathbb{R}^D} \sum_k p(\mathbf{X}=\mathbf{x}, K=k) \log_2 \times \frac{p(\mathbf{X}=\mathbf{x}, K=k)}{p(\mathbf{X}=\mathbf{x})p(K=k)}\, d\mathbf{x}. \quad (3)$$

However, even in this case, there might be an issue: profiling can be perfect (infinite amount of traces is available for a perfect estimation, no model assumption error, etc.), but the online matching traces might not coincide with the template, since the attack happens (in time) strictly after the characterization. In this case:

1) the profiling traces lead to a distribution $\hat{p}(\mathbf{X} = \mathbf{x}|K = k)$, abridged as $\hat{p}(\mathbf{x}|k)$; whereas,
2) the matching traces lead to a different distribution $\tilde{p}(\mathbf{x}|K)$.

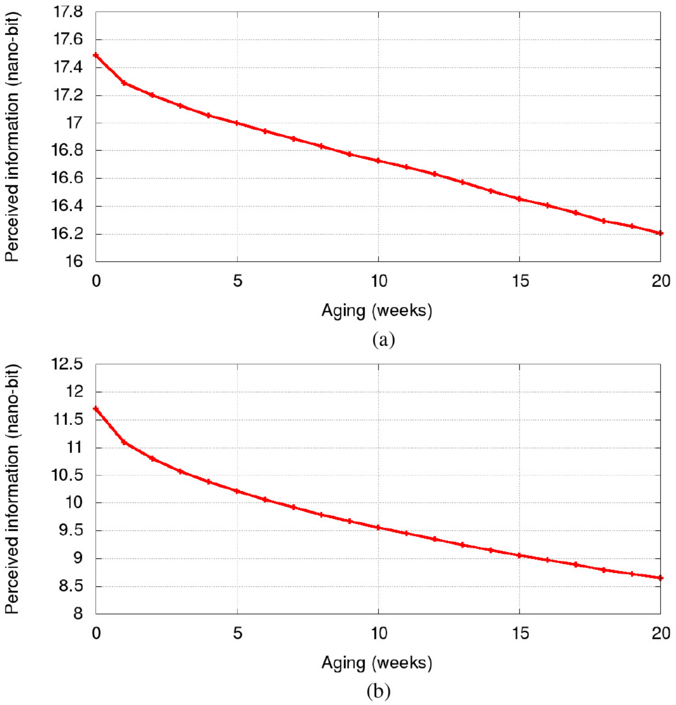
See the illustration in Fig. 13. This figure also depicts the difference between template $\hat{p}$ and attack $\tilde{p}$ where the difference increases with aging. In real setups, some measurement noise $N \sim \mathcal{N}(0, \sigma^2)$ is added on top of the averages shown in Fig. 13.

In such an asymmetric situation, the MI becomes the PI, as introduced in [51, eq. (3)]. The definition of MI is thus turned from (3) to (4)

$$\mathsf{PI}(\mathbf{X}, K) = \int_{\mathbf{x}\in\mathbb{R}^D} \sum_k \tilde{p}(\mathbf{x}, k) \log_2 \frac{\hat{p}(\mathbf{x}, k)}{\hat{p}(\mathbf{x})p(k)}\, d\mathbf{x}. \quad (4)$$

In this equation, the terms $\tilde{p}(\mathbf{x}, k) = \tilde{p}(\mathbf{x}|k)p(k)$ and $\hat{p}(\mathbf{x}, k) = \hat{p}(\mathbf{x}|k)p(k)$, where $p(k) = 2^{-2n}$ for the unprotected circuit (the sensitive variable is assumed to be uniformly distributed in transitions), can directly be deduced from the template and online estimated measurements.

The value $\hat{p}(\mathbf{x}) = \sum_k \hat{p}(\mathbf{x}, k) = \sum_k \hat{p}(\mathbf{x}|k)p(k) = (1/2^{2n}) \sum_k \hat{p}(\mathbf{x}|k)$ is a mixture of Gaussians. Hence, the integral in (4) is nontrivial, and shall be evaluated by numerical



(a)

(b)

Fig. 14. PI using (4) (Profiling Temperature = 105 °C, Attack Temperature = 105 °C, and σ = 0.001). (a) Unprotected S-box. (b) WDDL-protected S-box.

integration. Similarly, for the WDDL-protected design, we have $p(k) = 2^{-n}$ as all signals are initialized by "0" in the precharge phase.

Fig. 14(a) and (b) shows the PI for a template at age 0 and matching traces at age $0, 1, 2, \ldots, 20$ weeks for $\sigma = 0.001$.[4] Here, we assume that the noise is independent and identically distributed for each time sample $0 \leq d < D$. Thereby, (4) is simplified into a sum of 1-D-integrals:

$$\mathsf{PI}(\mathbf{X}, K) = \frac{1}{2^{2n}} \sum_{d=0}^{D-1} \int_{x_d=-\infty}^{+\infty} \sum_k \tilde{p}(x_d|k) \log_2 \frac{\hat{p}(x_d|k)}{\hat{p}(x_d)} \, \mathrm{d}x_d.$$

As Fig. 14 shows, starting from $\mathsf{PI}(\mathbf{X}, K) = \mathsf{MI}(\mathbf{X}, K)$ at equal aging (0 week), the PI decreases (slowly), and this decrease becomes less and less over time. Interestingly, this decrease is mirrored with respect to the SR of attacks shown in Fig. 8. This represents a known fact: the smaller the PI, the more traces needed to recover the key. Our results on the variation of the PI *vulnerability metric* due to aging corroborates the results from *actual attacks*. In particular, the strongest impact of aging is after a short period of time (one week) as the aging degradation is faster at first week; afterwards, the discrepancies continue to increase but at a slower rate. Comparing Fig. 14(a) and (b) depicts that as expected the PI for WDDL protected S-box is lower than the PI for the unprotected circuits when the circuits are new, e.g., 11.7 for the WDDL circuit compared to 17.5 for the unprotected one.

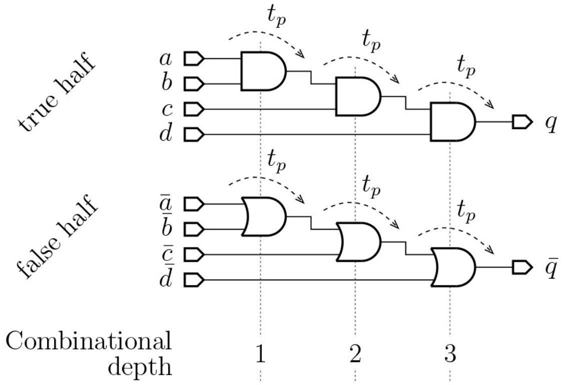


Fig. 15. Exemplar WDDL netlist where the early propagation effect is exacerbated owing to the large variability between gates input depth.

This result correspond to Fig. 6 and confirms that the number of traces required to reach $SR = 80\%$ would be more for the protected circuit. The decrease of PI is 7.3% for the unprotected circuit and 26.1% for the WDDL counterpart over the course of 20 weeks aging mismatches between the profiling and target circuits. the takeaway point from these observation is that aging misalignment between the profiling and target device hinders the template attack for both unprotected and WDDL-protected circuits. However, such effect is exacerbated in the WDDL-protected circuits.

VII. Interpretation of Our Results

Our results, regarding the attacks, show that aging and mismatch impede the attacker. In this section, we aim to provide a rationale which accounts for those facts.

First, let us recall that a prerequisite for WDDL resistance in front of side-channel attacks is that its netlist/layout is fully balanced, namely:

1) dual AND/OR gates have indistinguishable power consumption profile upon switching;
2) routing of their *true* q and *false* $\bar{q}$ outputs is also same.

In our experiments, the first property is only imperfectly satisfied (as is the case in real silicon), because AND and OR gates have their own power consumption profiles, and because on top of this (minor) discrepancy, we consider process variation. Notwithstanding, we ensured the second property rigorously, as we simulated the netlist before place-and-route.

But this is insufficient, insofar as WDDL suffers from the early evaluation effect, which causes input dependent leakage. More specifically, the number of toggles is an invariant, but the position in time of the toggles depends on the value of the inputs. Such leakage is nonetheless hard to model, thereby we resort to "template attacks" in the article. Fig. 15 can serve as an illustration of this phenomenon: it depicts the function $q = \mathrm{AND}(a, b, c, d)$, complemented with its dual $\bar{q} = \mathrm{OR}(\bar{a}, \bar{b}, \bar{c}, \bar{d})$. This figure leverages the simple WDDL concepts presented earlier in Section II-C. Let us denote by t_p the propagation time through any of the AND or OR gates. Upon precharge phase, all inputs are reset, namely, $a = b = c = d = \bar{a} = \bar{b} = \bar{c} = \bar{d} = 0$. As a consequence of the "wave" effect of WDDL logic style, all internal nodes

[4] The value $\sigma = 0.001$ allows for fast computation of integrations involved in the PI expression (4); larger values, e.g., $\sigma = 0.016/0.032$ would nonetheless yield evolution of PI with aging similar to that represented in Fig. 14.

are also at 0, including the outputs $q = \bar{q} = 0$. Let us now analyze what happens upon evaluation, for two opposite valid inputs.

1) We first assume that a, b, c and d take $a = b = c = d = 1$ (hence $\bar{a}$, $\bar{b}$, $\bar{c}$, $\bar{d}$ remain at 0, i.e., $\bar{a} = \bar{b} = \bar{c} = \bar{d} = 0$). Then, the AND gate driven by a and b toggles first. Thus, only after a duration equal to t_p, the second AND gate can toggle. And similarly, only after another t_p amount of time, the last AND gets at its input two ones, hence can toggle. In the dual netlist portion, there is no activity. Therefore, the power consumption consists in three gates toggle, one initially at time $t = 0$, a second one at time $t = t_p$ and a third one at time $t = 2t_p$.
2) Second, we assume that a, b, c, and d take $a = b = c = d = 0$ (hence $\bar{a}$, $\bar{b}$, $\bar{c}$, $\bar{d}$ change values to 1, i.e., $\bar{a} = \bar{b} = \bar{c} = \bar{d} = 1$). There is no change in values at the entrance of the true netlist part (that which is made up of AND gates), hence, no toggle. On the contrary, in the false netlist part, all OR gates have at least one input transitioning from 0 to 1. Consequently, they can all evaluate to 1 at once. Incidentally, this is their final value (there is no glitch in a WDDL netlist). As a summary, the complete netlist features three toggles, occurring simultaneously at time $t = 0$.

This example underlines two important facts about early evaluation effect (see also [31]).

1) The early propagation effect can accumulate along the paths; in the previous example, when evaluating at $a = b = c = d = 1$, the last AND gate toggles later than the first AND gate owing to the fact the last gate needs to wait for the first gate to evaluate. Therefore, the deeper and the more unbalanced the delays in the netlists, the more chaotic the early propagation effect, and the more misaligned the power traces. This comment applies particularly to our use case depicted in Fig. 3(b), as it has multiple paths of varied length.
2) The early propagation effect can be all the better observed (e.g., by an attacker) as the propagation time t_p is larger, since the different contributions of constituent gates is more clearly standing out.

Let us now apply those findings in the context of our study. Aging has two contradictory effects on WDDL leakage:

1) as shown in Fig. 5, aging spreads the activity over time, thereby allowing, from the attacker point of view, a better discrimination of early propagation gate toggles;
2) but also, the power profiles depart more and more from the learnt ones, thus reducing the SR of attacks.

Our results show that the latter effect is stronger than the former, in which attacks do become more difficult with aging.

As expected, the process variation increases the imbalance between the template device and the profile device, thus making the attack more difficult to succeed, as shown in Fig. 10. As stated before, the aging amplifies this phenomenon and adds security, especially with WDDL logic as the increase in number of traces is faster with WDDL. However, it has to be recalled that nonprofiled side-channel attacks can take advantage of a bigger imbalance between the WDDL gates and the early evaluation effect, as the leakage increases with aging. Besides aging, the increase of delay due to temperature has a significant impact on the attack. This is particularly true for WDDL protected devices as the attack can definitely fail for different temperature conditions between template and target devices as shown in Fig. 12(b).

Eventually, let us note that we have carried out DPA in another research, focusing on SABL [52], which is another hiding countermeasure based on power equalization (like WDDL, but without early evaluation). SABL features well synchronized pairs of signals; hence, aging exacerbates the tiny differences between the two signals in a pair. The situation is different in WDDL, as no realistic model can be derived. Therefore, correlation attacks are not considered in our case studies.

VIII. Conclusion

Internet-of-Things (IoT) applications require embedded cryptographic accelerators for allowing the secure device connectivity and remote management. This article investigated the impact of transistor aging on the SR of the template attack. We addressed how the aging-related change of device specifications can adversely affect the success of a template attack when there is an aging mismatch between the device used for characterization and the target device. The results of launching a template attack on the S-box module of the PRESENT cipher showed that the traces needed to reach 80% SR increases in the order of 23% in a course of 20 weeks at 105 °C for an unprotected device. Such increase is around 112% if the target circuit is WDDL-protected. Therefore, aging increases leakage but, at the same time, induces traces misalignments. All in one, we showed that the attacks are basically impeded more than fostered. To increase the SR of the attack, the operational environment, including supply voltage, clock signal shape, etc., must be the same for the training and matching devices. In particular the temperature mismatch between profiling and target device should be avoided. Avoiding such mismatch is extremely crucial for attacking WDDL circuits. As the secondary factor, aging should be also balanced to fine tune the attack. The technological dispersion accounts for more traces needed to break the aged unprotected and WDDL-protected devices, while the latter is affected more by such process mismatch.

Note that the security of devices can be estimated by quotations, e.g., depending on the time to profile, the time to break, the cost of the measurement tool, the expertise of the evaluator, etc. This level should be selected according to the value of the protected assets. It is noteworthy to mention that the security of a device should be a timely property, meaning that the attacker is assumed to be able to strike at any time, including right after the product is released (age $t = 0$). As we consider, in this article, the security level along the product life cycle, we have not restricted ourselves to the security in the long run, but consistently over the product deployment period (age $= 0$ to lifetime).

References

[1] O. Sinanoglu *et al.*, “Reconciling the IC test and security dichotomy,” in *Proc. 18th IEEE Eur. Test Symp. (ETS)*, 2013, pp. 1–6.

[2] S. Khan, N. Z. Haron, S. Hamdioui, and F. Catthoor, "NBTI monitoring and design for reliability in nanoscale circuits," in *Proc. DFTS*, 2011, pp. 68–76.

[3] H. Kufluoglu and M. A. Alam, "A generalized reaction-diffusion model with explicit H-H2 dynamics for negative-bias temperature-instability (NBTI) degradation," *IEEE Trans. Electron Devices*, vol. 54, no. 5, pp. 1101–1107, May 2007.

[4] Y. Lu, L. Shang, H. Zhou, H. Zhu, F. Yang, and X. Zeng, "Statistical reliability analysis under process variation and aging effects," in *Proc. ACM/IEEE Design Autom. Conf.*, 2009, pp. 514–519.

[5] D. Saha, D. Varghese, and S. Mahapatra, "Role of anode hole injection and valence band hole tunneling on interface trap generation during hot carrier injection stress," *IEEE Electron Device Lett.*, vol. 27, no. 7, pp. 585–587, Jul. 2006.

[6] R. Rodriguez, J. Stathis, and B. Linder, "Modeling and experimental verification of the effect of gate oxide breakdown on CMOS inverters," in *Proc. IEEE Int. Rel. Phys. Symp.*, 2003, pp. 11–16.

[7] N. Karimi, A. K. Kanuparthi, X. Wang, O. Sinanoglu, and R. Karri, "MAGIC: Malicious aging in circuits/cores," *ACM Trans. Archit. Code Optim.*, vol. 12, no. 1, pp. 1–25, 2015.

[8] P. C. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Advances in Cryptology (CRYPTO)* (Lecture Notes in Computer Science), vol. 1666, M. J. Wiener, Ed. Berlin, Germany: Springer, 1999, pp. 388–397.

[9] L. De Meyer, O. Reparaz, and B. Bilgin, "Multiplicative masking for AES in hardware," *IACR Trans. Cryptogr. Hardw. Embedded Syst.*, vol. 2018, no. 3, pp. 431–468, 2018.

[10] E. Trichina, "Combinational logic design for AES SubByte transformation on masked data," in *IACR Cryptol. EPrint Arch.*, vol. 2003, p. 236, 2003.

[11] P. Kocher, J. Jaffe, B. Jun, and P. Rohatgi, "Introduction to differential power analysis," *J. Cryptogr. Eng.*, vol. 1, no. 1, pp. 5–27, 2011.

[12] É. Brier, C. Clavier, and F. Olivier, "Correlation power analysis with a leakage model," in *Cryptographic Hardware and Embedded Systems*. Berlin, Germany: Springer, 2004, pp. 16–29.

[13] B. Gierlichs, L. Batina, P. Tuyls, and B. Preneel, "Mutual information analysis," in *Cryptographic Hardware and Embedded Systems*. Berlin, Germany: Springer, 2008, pp. 426–442.

[14] S. Chari, J. R. Rao, and P. Rohatgi, "Template attacks," in *Cryptographic Hardware and Embedded Systems*. Berlin, Germany: Springer, 2002, pp. 13–28.

[15] S. Picek, A. Heuser, and S. Guilley, "Template attack vs bayes classifier," *IACR Cryptol. ePrint Arch.*, vol. 2017, p. 531, 2017.

[16] N. Karimi, S. Guilley, and J.-L. Danger, "Impact of aging on template attacks," in *Proc. Great Lakes Symp. VLSI (GLSVLSI)*, 2018, pp. 455–458.

[17] K. Tiri and I. Verbauwhede, "Securing encryption algorithms against DPA at the logic level: Next generation smart card technology," in *Cryptographic Hardware and Embedded Systems*. Berlin, Germany: Springer, 2003, pp. 125–136.

[18] K. K. Kim, "On-chip delay degradation measurement for aging compensation," *Indian J. Sci. Technol.*, vol. 8, no. 8, p. 777, 2015.

[19] F. Oboril and M. B. Tahoori, "ExtraTime: Modeling and analysis of wearout due to transistor aging at microarchitecture-level," in *Proc. DSN*, 2012, pp. 1–12.

[20] M. T. H. Anik, S. Guilley, J.-L. Danger, and N. Karimi, "On the effect of aging on digital sensors," in *Proc. VLSI Design Conf. (VLSID)*, 2020, pp. 189–194.

[21] S. Zafar *et al.*, "A comparative study of NBTI and PBTI (charge trapping) in SiO2/HfO2 stacks with FUSI, TiN, Re gates," in *Proc. Symp. VLSI Technol.*, 2006, pp. 23–25.

[22] *HSPICE User Guide: Basic Simulation and Analysis*, Synopsys, Mountain View, CA, USA, 2016.

[23] W. Wang, S. Yang, S. Bhardwaj, S. Vrudhula, F. Liu, and Y. Cao, "The impact of NBTI effect on combinational circuit: Modeling, simulation, and analysis," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 18, no. 2, pp. 173–183, Feb. 2010.

[24] A. Heuser, S. Picek, S. Guilley, and N. Mentens, "Side-channel analysis of lightweight ciphers: Does lightweight equal easy?" in *Proc. Int. Workshop Radio Freq. Identification IoT Security (RFIDSec)*, 2016, pp. 91–104.

[25] A. Bogdanov *et al.*, "PRESENT: An ultra-lightweight block cipher," in *Cryptographic Hardware and Embedded Systems*. Berlin, Germany: Springer, 2007, pp. 450–466.

[26] Y. Fei, A. A. Ding, J. Lao, and L. Zhang, "A statistics-based success rate model for DPA and CPA," *J. Cryptogr. Eng.*, vol. 5, no. 4, pp. 227–243, 2015.

[27] D. Bellizia, G. Scotti, and A. Trifiletti, "Implementation of the PRESENT-80 block cipher and analysis of its vulnerability to Side Channel Attacks Exploiting Static Power," in *Proc. Int. Conf. Mixed Design Integr. Circuits Syst.*, 2016, pp. 211–216.

[28] A. Heuser, S. Picek, S. Guilley, and N. Mentens, "Lightweight ciphers and their side-channel resilience," *IEEE Trans. Comput.*, vol. 69, no. 10, pp. 1434–1448, Oct. 2020.

[29] D. Canright, "A very compact S-box for AES," in *Cryptographic Hardware and Embedded Systems*. Berlin, Germany: Springer, 2005, pp. 441–455.

[30] K. Tiri and I. Verbauwhede, "A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation," in *Proc. Design Autom. Test Europe (DATE)*, 2004, pp. 246–251.

[31] D. Suzuki and M. Saeki, "An analysis of leakage factors for dual-rail pre-charge logic style," *IEICE Trans. Fund. Electron. Commun. Comput. Sci.*, vol. 91-A, no. 1, pp. 184–192, 2008.

[32] S. Guilley, L. Sauvage, J.-L. Danger, and P. Hoogvorst, "Area optimization of cryptographic co-processors implemented in dual-rail with precharge positive logic," in *Proc. Int. Conf. Field Program. Logic Appl.*, 2008, pp. 161–166.

[33] N. Selmane, S. Bhasin, S. Guilley, T. Graba, and J.-L. Danger, "WDDL is protected against setup time violation attacks," in *Proc. 6th Int. Workshop Fault Diagn. Tolerance Cryptogr.*, 2009, pp. 73–83.

[34] S. Guilley, L. Sauvage, J.-L. Danger, T. Graba, and Y. Mathieu, "Evaluation of power-constant dual-rail logic as a protection of cryptographic applications in FPGAs," in *Proc. Int. Conf. Secure Syst. Integr. Rel. Improvement (SSIRI)*, 2008, pp. 16–23.

[35] L. Sauvage, S. Guilley, J.-L. Danger, Y. Mathieu, and M. Nassar, "Successful attack on an FPGA-based WDDL DES cryptoprocessor without place and route constraints," in *Proc. Design Autom. Test Europe (DATE)*, 2009, pp. 640–645.

[36] É. de Chérisey, S. Guilley, A. Heuser, and O. Rioul, "On the optimality and practicability of mutual information analysis in some scenarios," *Cryptogr. Commun.*, vol. 10, no. 1, pp. 101–121, 2018. [Online]. Available: https://doi.org/10.1007/s12095-017-0241-x

[37] P. C. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems," in *Advances in Cryptology (CRYPTO)* (Lecture Notes in Computer Science), vol. 1109. Berlin, Germany: Springer, 1996, pp. 104–113.

[38] K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic analysis: Concrete results," in *Cryptographic Hardware and Embedded Systems*. Berlin, Germany: Springer, 2001, pp. 251–261.

[39] N. Bruneau, S. Guilley, A. Heuser, D. Marion, and O. Rioul, "Optimal side-channel attacks for multivariate leakages and multiple models," *J. Cryptogr. Eng.*, vol. 7, no. 4, pp. 331–341, 2017.

[40] T. Korak, M. Hutter, B. Ege, and L. Batina, "Clock glitch attacks in the presence of heating," in *Proc. Workshop Fault Diagn. Tolerance Cryptogr. (FDTC)*, 2014, pp. 104–114.

[41] F. Durvaux, F. Standaert, and N. Veyrat-Charvillon, "How to certify the leakage of a chip?" in *Proc. Int. Conf. Theory Appl. Cryptogr. Techn. (EUROCRYPT)*, 2014, pp. 459–476.

[42] S. Wang, J. Chen, and M. Tehranipoor, "Representative critical reliability paths for low-cost and accurate on-chip aging evaluation," in *Proc. Int. Conf. Comput.-Aided Design (ICCAD)*, 2012, pp. 736–741.

[43] *Nangate 45nm Open Cell Library*. Accessed: May, 2016. [Online]. Available: http://www.nangate.com

[44] N. Courtois, D. Hulme, and T. Mourouzis, "Solving circuit optimisation problems in cryptography and cryptanalysis," *IACR Cryptol. ePrint Arch.*, vol. 2011, p. 475, 2011.

[45] A. Heuser, O. Rioul, and S. Guilley, "Good is not good enough—Deriving optimal distinguishers from communication theory," in *Cryptographic Hardware and Embedded Systems*. Berlin, Germany: Springer, 2014, pp. 55–74.

[46] C. Carlet, J.-L. Danger, S. Guilley, H. Maghrebi, and E. Prouff, "Achieving side-channel high-order correlation immunity with leakage squeezing," *J. Cryptogr. Eng.*, vol. 4, no. 2, pp. 107–121, 2014.

[47] S. Guilley, A. Heuser, and O. Rioul, "A key to success: Success exponents for side-channel distinguishers (extended version of [15])," Cryptol. ePrint Arch., Lyon, France, Rep. 2016/987, 2016.

[48] S. Bhasin, J.-L. Danger, S. Guilley, and Z. Najm, "Side-channel leakage and trace compression using normalized inter-class variance," in *Proc. Workshop Hardw. Archit. Support Security Privacy*, 2014, pp. 1–9.

[49] M. Elaabid and S. Guilley, "Portability of templates," *J. Cryptogr. Eng.*, vol. 2, no. 1, pp. 63–74, 2012.

[50] L. Batina, B. Gierlichs, E. Prouff, M. Rivain, F.-X. Standaert, and N. Veyrat-Charvillon, "Mutual information analysis: A comprehensive study," *J. Cryptol.*, vol. 24, no. 2, pp. 269–291, 2011.

[51] M. Renauld, F. Standaert, N. Veyrat-Charvillon, D. Kamel, and D. Flandre, "A formal study of power variability issues and side-channel attacks for nanoscale devices," in *Proc. Int. Conf. Theory Appl. Cryptogr. Techn. (EUROCRYPT)*, 2011, pp. 109–128.

[52] M. T. H. Anik, B. Fadaeinia, A. Moradi, and N. Karimi, "On the impact of aging on power analysis attacks targeting power-equalized cryptographic circuits," in *Proc. ASP-DAC*, 2021, pp. 414–420.

Farzad Niknia (Student Member, IEEE) received the B.Sc. and M.Sc. degrees in electrical and electronics engineering from the University of Tabriz, Tabriz, Iran, in 2014 and 2018, respectively. He is currently pursuing the Ph.D. degree in computer engineering with Northeastern University, Boston, MA, USA.

He worked as a Research Assistant with IC Design Laboratory through the M.Sc. degree. He joined the Secure, Reliable, and Trusted Systems Research Laboratory (SECRETS LAB), University of Maryland Baltimore County, Baltimore, MD, USA, in 2019, and continued his research there particularly on hardware Trojan detection and side-channel power analysis attacks. He is currently a Research Assistant with a concentration on ASIC Design at Northeastern University. His research interests include ASIC and FPGA design, VLSI, EDA tools, design for test, and hardware security.

Jean-Luc Danger (Member, IEEE) received the Engineering degree in electrical engineering from the École Supérieure d'Électricité, Gif-sur-Yvette, France, in 1981.

He is a Full Professor with TELECOM Paris, Paris, France. 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 has authored more than 250+ scientific publications and patents in architectures of embedded systems and security, and is the cofounder and scientific advisor of the Secure-IC Company. After 12 years in industrial laboratories (PHILIPS, Eindhoven, The Netherlands, and NOKIA, Espoo, Finland), he joined TELECOM ParisTech in 1993, where he became a Full Professor in 2002. His personal research interests are trusted computing, cybersecurity, random number generation, and protected implementations in novel technologies.

Sylvain Guilley (Member, IEEE) received the Engineer degree from École Polytechnique, Palaiseau, France, in 2000, and Télécom-Paris, Paris, France, in 2002, the M.Sc. degree in quantum physics from École Normale Supérieure, Paris, France, in 2002, the Ph.D. degree from Télécom-Paris in 2007, and the Accreditation to Supervise Research (French "HDR") degree from Paris VII University, Paris, in 2012.

He is currently the General Manager and the CTO with Secure-IC, a company offering security for embedded systems. Secure-IC's flagship product is the multicertified SECURYZR integrated Secure Element (iSE). The iSE is part of the integrated Secure Services Platform aiming at managing iSE with IoTs from the cloud. Within Secure-IC, he is also the Director of "Threat Analysis" and "Think Ahead" business lines, which develop, respectively, security evaluation tools and advanced research. He is also a Professor with TELECOM-Paris, Paris, France, an Associate Research with École Normale Supérieure, Paris, and an Adjunct Professor with the Chinese Academy of Sciences, Beijing, China. He is an Alumni of Ecole Polytechnique, Palaiseau, France, and TELECOM-ParisTech. He has coauthored over 250 research papers and filed over 40 patents. His research interests are trusted computing, cyber–physical security, secure prototyping in FPGA and ASIC, and formal/mathematical methods.

Dr. Guilley is an Associate Editor of the *Journal of Cryptography Engineering* (Springer). He is a member of the IACR and a Senior Member of CryptArchi club. Since 2012, he has been organizes the PROOFS workshop, which brings together researchers whose objective is to increase the trust in the security of embedded systems. He is also the Lead Editor of international standards, such as ISO/IEC 20897 (Physically Unclonable Functions), ISO/IEC 20085 (Calibration of noninvasive testing tools), and ISO/IEC 24485 (White Box Cryptography). He is "High Level Principles for Design/Architecture" Team Leader for the drafting of Singapore TR68 standard on Cyber-Security of Autonomous Vehicles.

Naghmeh Karimi (Member, IEEE) received the B.Sc., M.Sc., and Ph.D. degrees in computer engineering from the University of Tehran, Tehran, Iran, in 1997, 2002, and 2010, respectively.

She was a Visiting Researcher with Yale University, New Haven, CT, USA, from 2007 to 2009, and a Postdoctoral Researcher with Duke University, Durham, NC, USA, from 2011 to 2012. She has been a Visiting Assistant Professor with the New York University, New York, NY, USA, and Rutgers University, New Brunswick, NJ, USA, from 2012 to 2016. She joined the University of Maryland Baltimore County, Baltimore, MD, USA, as an Assistant Professor in 2017, where she leads the Secure, Reliable and Trusted Systems Research Laboratory. She has published three book chapters and authored/coauthored more than 50 papers in referred conference proceedings and journal manuscripts. Her current research interests include hardware security, VLSI testing, design-for-trust, design-for-testability, and design-for-reliability.

Dr. Karimi is a recipient of the National Science Foundation CAREER Award in 2020. She serves as an Associate Editor for the *Journal of Electronic Testing: Theory and Applications* (Springer). She is also the Corresponding Guest Editor of the *Emerging and Selected Topics in Circuits and Systems*; special issue in Hardware Security in Emerging Technologies.