IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 29, 2021, accepted June 3, 2021, date of publication June 21, 2021, date of current version June 30, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3090752

Masked SABL: A Long Lasting Side-Channel Protection Design Methodology

BIJAN FADAEINIA[1], MD TOUFIQ HASAN ANIK[2], (Graduate Student Member, IEEE), NAGHMEH KARIMI[2], (Member, IEEE), AND AMIR MORADI[1]

[1]Ruhr University Bochum, Horst Görtz Institute for IT Security, 44801 Bochum, Germany
[2]Computer Science and Electrical Engineering Department, University of Maryland Baltimore County, Baltimore, MD 21250, USA

Corresponding author: Bijan Fadaeinia (bijan.fadaeinia@rub.de)

This work was supported in part by the Deutsche Forschungsgemeinschaft (DFG) through the Germany's Excellence Strategy under Grant EXC 2092 CASA-390781972, in part by the Project "Aged but Fit: Long Lasting Security for Trusted Platforms" under Grant 418658052, and in part by the National Science Foundation, Faculty Early Career Development (CAREER) Award through the Project "Investigating the Impact of Device Aging on the Security of Cryptographic Chips" under Grant NSF CNS-1943224.

ABSTRACT As an outstanding cell-level countermeasure to defeat power analysis attacks, dual-rail pre-charge logics rely on balanced complementary paths. During the circuit lifetime, the gates undergo unavoidable changes due to the so-called device aging, hence imbalancing the dual rails. Here, we focus on Sense Amplifier Based Logic (SABL), and highlight the vulnerability of corresponding circuits when the device is aged. By integrating gate-level masking, we introduce a modified variant of SABL, maintaining its resistance in presence of device aging. The corresponding results, covering both dynamic and static power profiles, show the prominent impact of our construction on extending the protection of circuits for their entire lifetime.

INDEX TERMS Cryptographic circuits, device aging, Sense Amplifier Based Logic (SABL), side-channel analysis (SCA).

I. INTRODUCTION

Cryptographic circuits offer continued advances in authenticating messages and devices as well as preserving the integrity and confidentiality of sensitive information through implementation of cryptographic algorithms in hardware. The deployment of such devices in military, space, finance and other critical applications that require a high level of security is inevitable. Although developed to maintain security and trust, the physical implementation of cryptographic devices can be compromised by the adversaries who aim at extracting the sensitive information these circuits conceal. Accordingly, preserving the security of these devices is of utmost importance.

Revealing the key of the cryptographic devices leading to recovering the corresponding encrypted data has been always an attractive task for adversaries, particularly with the rising inclusion of smart cards in everyday life. Although traditionally, the security of a cryptographic device depends on the complexity of the underlying cryptographic algorithm and the deployed authentication protocol, an adversary may benefit from the information collected by monitoring its physical characteristics. Such so-called Side-Channel Analysis (SCA) attacks, are conducted by analyzing e.g., running time, power consumption, and electromagnetic radiation of the underlying cryptographic device during its operations. In practice, dependency between the side-channel information and the device intermediate values during the encryption/decryption can reveal the deployed key [17].

To thwart such attacks, different countermeasures have been proposed in literature which can be mainly categorized to two groups of *masking* and *hiding*. In practice, masking countermeasures try to randomize the intermediate values via a form of secret-sharing scheme, while hiding countermeasures opt to reduce the dependency of power consumption on processed data via reducing the Signal-to-Noise Ratio (SNR) [17].

DPA-resistant logic styles (where DPA refers to Dynamic Power Analysis [13]), as a well-known class of hiding countermeasures, try to equalize the power consumption of the target cryptographic circuit independent of processed data. Obviously, this cannot be fully achieved due to process

The associate editor coordinating the review of this manuscript and approving it for publication was Mehdi Sookhak.

variation, but the SNR can be significantly lowered thereby hardening the implementations against power SCA attacks. Some of such techniques are based on conventional standard cells [5], [29] and some others require full-custom cell design [6], [28]. Sense Amplifier Based Logic (SABL) is among such countermeasures which provides a reasonable trade-off between the overhead and achieved security level. The resistance of such logic styles, including SABL, are based on a balance between the rising (resp. falling) time of dual rails representing complementary signals. However, due to the so-called device aging, the specifications of the transistors building a digital circuit change over time, e.g., their threshold voltage. The transistors' threshold voltage is among such specifications, whose change naturally affects the gates' timing characteristics, hence deviating from the aforementioned balance [4]. Therefore, although SABL-based circuits have been shown effective against SCA attacks, such a resistance may not be maintained over the circuits' lifetime [4]. More precisely, the adversary can intentionally accelerate the aging process and make use of the resulting SCA leakage to recover the embedded secret.

To alleviate this shortcoming, and sustain the security of such protected circuits even when they have been used for a while, an aging-resilient countermeasure is needed. Accordingly, this paper targets SABL, and investigates the vulnerability of corresponding circuits after being aged. We even move one step further by presenting a solution which keeps the same level of SCA resistance when the device is aged. To achieve our goals, we construct a new variant of SABL, i.e., masked SABL, by making use of the concept behind masked dual-rail logic, where the rails (of dual-rail routes) are randomly swapped during the operation of the circuit. To our best knowledge, no aging-resilient countermeasure against SCA attacks has been proposed in open literature.

In this paper, we investigate the effect of aging on the success of SCA attacks, which exploit *static* power consumption, as well as those which monitor the circuit's *dynamic* power. Accordingly, we demonstrate the robustness of our new construction in preventing both static and dynamic power SCA leakages in presence of device aging. To this end, after giving the essential background in Section II, we discuss the impact of aging in degrading the balancedness of SABL cells in Section III. Then we present our new aging-resilient structure in Section IV. We further construct a transistor-level description of the PRESENT S-box (as the most complex part of the corresponding encryption function), and run extensive transistor-level simulations (using HSpice MOSRA) in Section V to emulate the device aging and evaluate the vulnerability/resistance of both corresponding SABL and masked SABL circuits against static and dynamic power analysis attacks. At the end, Section VI concludes the conducted research.

II. BACKGROUND

In the following, we shortly give the basics of underlying logic style SABL, and that of CMOS device aging.

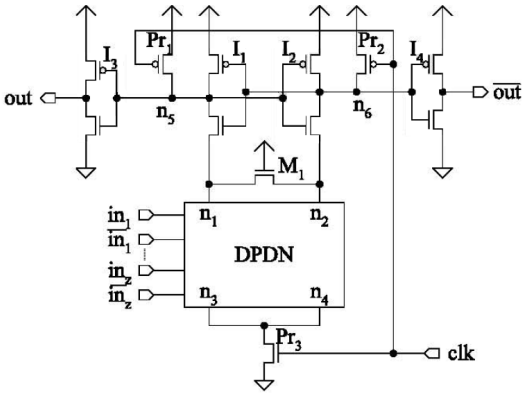


FIGURE 1. General structure of an SABL cell, taken from [17].

A. SENSE AMPLIFIER BASED LOGIC

SABL [28], [31] is a Dual-Rail Pre-charge (DRP) logic style that carries both input and output signals on complementary wires. As Figure 1 depicts, each SABL cell includes two cross-coupled inverters and a differential pull-down network (DPDN). While other parts of the circuit are the same for every SABL cell, the DPDN is responsible for the functionality of the cell and is made of only NMOS transistors. Each SABL cell has two operational phases: *pre-charge* and *evaluation*. In the pre-charge phase, `clk` is low, hence nodes n_5 and n_6 are set to high. Therefore, at the end of this phase, output signals `out` and $\overline{out}$ are pre-charged to low. The same holds for the input signals as they are driven by preceding SABL cells (or the circuit's primary inputs). At the beginning of the evaluation phase, i.e., positive edge of `clk`, the SABL cell (through the DPDN) starts evaluating the output once all its dual-rail inputs are complementary. During this phase, all internal nodes of DPDN go to low, while only one of the complementary outputs `out` and $\overline{out}$ goes high, depending on which node n_1 and n_2 goes low earlier. This way, no glitch happens in either internal or output signals, and for each clock cycle, it is guaranteed to have only one falling transition at the start of the pre-charge phase, and only one rising transition during the evaluation phase. Supposing a balance between capacitive load of dual rails, dynamic power consumption of each cell (resp. the circuit) should be independent of processed data.

Following [31], DPDN should fulfill some requirements:

- It should be always-connected, i.e., all its internal nodes should be charged in the pre-charge phase and discharged during the evaluation phase.
- It should be balanced, i.e., all possible paths to GND should have equivalent resistance. Hence, each route should include an equal number of transistors with identical parameters.
- Each complementary input should be connected to the same number of transistors, thereby balancing their capacitive load.
- Each SABL cell should evaluate when all its inputs are set to complementary values to avoid data-dependent time-of-evaluation [17].

If any of these requirements is not maintained, the security of the resulting circuit cannot be guaranteed.

B. AGING MECHANISMS

Due to the device aging, the performance of a circuit degrades over time, and eventually it fails to meet its frequency requirements [2], [21]. Among all aging mechanisms, Bias Temperature-Instability (BTI) and Hot Carrier Injection (HCI) are two leading factors in circuit degradation over time [3], [11].

The BTI (including Negative and Positive BTI referred to as NBTI and PBTI, respectively) results in an increase in the threshold voltage (V_{th}) of transistors over time. NBTI and PBTI occur in PMOS and NMOS transistors, respectively. The impact of NBTI is more dominant than PBTI beyond the 45 nm technology node. However, PBTI effects have also received significant attention in smaller technology nodes [32].

A PMOS transistor experiences two phases of NBTI. The *stress* phase occurs when the transistor is ''on'' ($V_{gs} < V_{th}$). In this phase, the positive interface traps are generated at the Si-SiO_2 interface resulting in V_{th} increase. In the second phase (i.e., *recovery*) which occurs when the transistor is ''off'', the V_{th} drift is partially recovered. The BTI effects depend on the specification of the transistor under-stress, supply voltage, temperature, and stress time [11]. The last three parameters (which are actually external) can be used to accelerate the aging. The NBTI effect is high in the first couple of weeks but the V_{th} tends to saturate for long stress times. The PBTI affects NMOS transistors in a similar way that NBTI affects PMOS transistors.

Figure 2 shows the V_{th} drift of a PMOS transistor continuously under stress for 6 months and the one alternating stress/recovery phases every other month. As shown, NBTI effect is high in the beginning but the threshold voltage tends to saturate for long stress times. The impact is exacerbated with thinner gate oxide and higher operating temperature [1].

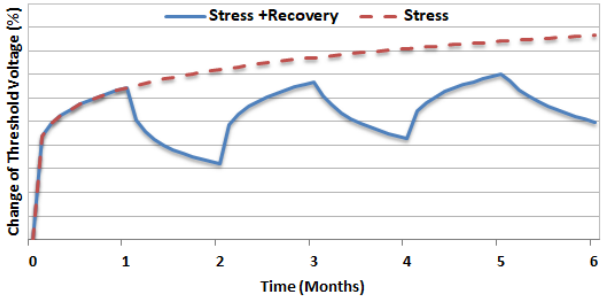


FIGURE 2. NBTI-induced threshold-voltage shift of a PMOS transistor over time [10]. Y-axis values are not shown to make the graph generic for different technologies.

HCI occurs when hot carriers are injected into the gate dielectric during transistor switching and remain there. HCI is a function of switching activity, and results in shifting the threshold voltage and the drain current of transistors under stress [24]. HCI depends on temperature, clock frequency, usage time, and activity factor of the transistor under stress, i.e., the percentage of cycles in which the transistor is switching [21]. Unlike BTI, HCI does not have any recovery phase.

III. CONCEPT

A. INFORMATION LEAKAGE IN SABL

Side-channel data leakage is an unintended dependency between externally-measurable characteristics of a device such as power consumption and its processed data. Such a dependency can be observed in both dynamic [13] and static power [18]. In advanced semiconductor technologies the leakage current increase due to lower threshold voltages, shorter channel lengths, and thinner gate oxides, results in higher static power side-channel leakage [9]. On the other hand, decrease of supply voltage and parasitic capacitances in such new technologies have led to lower dynamic power consumption in the new generation of integrated circuits. In the case of SABL, the most important source of information leakage through dynamic power is an imbalance between complementary rails, including their loads and path delays [17]. In contrast, dependency of static power (leakage current) to the value of the circuit's signals generally relies on source-drain current I_{sd}, gate-source current I_{gs}, and gate-drain current I_{gd} of off-state transistors as well as I_{gs} and I_{gd} of on-state transistors [9].

Since all inputs and outputs of an SABL cell are low during the pre-charge phase, its information leakage through static power can only be relevant in the evaluation phase, i.e., when `clk` is high and all its inputs are complementary and stable. In this state, all n_1 to n_4 nodes and consequently all internal nodes of DPDN are connected to GND (see Figure 1). Therefore, source and drain of all NMOS transistors in DPDN are connected to GND, hence having only I_{gs} and I_{gd} passing through the transistors' gate to GND. As stated in Section II-A with respect to the DPDN's requirements, for every input combination, the same number of transistors in DPDN is in on- or off-state. Hence, ignoring process variation, the DPDN's leakage current is expected to be just slightly different for various inputs. On the other hand, the leakage current of the cross-coupled inverters is almost due to I_{sd}, which is actually the dominant part of static power. Since the cross-coupled inverters are ideally symmetric, their leakage current is also independent of the inputs. As a result, in an ideal SABL cell, we expect no dependency between the circuit's static power and its inputs. However, in practice due to process variation, the circuit faces some asymmetry affecting its information leakage via both dynamic and static power profiles.

B. AGING-INDUCED DELAY CHANGE

By the first set of experiments, we shortly examine the effect of NBTI aging on the propagation delay of primitive logic gates. To this end, we simulated different standard and SABL

gates and observed their propagation delay when aged over a period of 6 months. For the simulations, we made use of Synopsys Hspice and MOSRA level 3 model to simulate the aging effects. Both HCI and BTI flags have been activated. As a side note, in our simulations we did not consider any parasitic capacitances originating from the layout. However, those which are made by the topology of the circuit (fanouts and fanins) are inherently covered. Figure 3 shows the corresponding results for each classic (i.e., unprotected) primitive logic gate as well as their SABL-protected counterpart over time when these gates are fed with randomly generated inputs between 1 and 6 months.

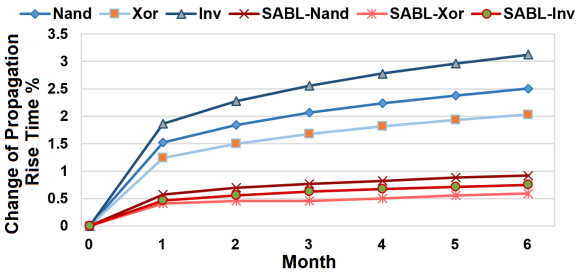


FIGURE 3. Change of propagation rise time (%) of basic gates with different aging conditions.

As shown in Fig. 3, each primitive gate experiences different amount of delay change related to its transistor level topology. This observation confirms that each path in a cryptographic device may degrade with a different rate based on the type of its underlying gates, and the input values feeding it. The takeaway point from this observation is that aging can result in imbalances in the power consumption of each gate, each path, and in sum in the total power consumption of a device during the time even if the device is equipped with power-equalization schemes. These imbalances may improve the success of the SCA attacks on such protected devices.

C. EFFECT OF AGING ON SABL

As expressed in Section II-B, BTI and HCI are the aging mechanisms with the most influence on degradation of the digital circuits' performance, particularly on the transistors' threshold voltage. As stated in Section II-A, from security perspective, symmetry between the characteristics of complementary dual-rail signals is the most crucial requirement of DRP logics. Focusing on SABL, any degradation in this symmetry (due to the aging-induced threshold voltage drift and drain's current reduction) is expected to lead to an increase in information leakage through both static and dynamic power. In order to evaluate this prediction, we conducted simulations based on a 4-bit S-box of the PRESENT cipher [7]. More precisely, we constructed the transistor-level representation of the S-box implemented by SABL gates, formed only by inverter and 2-input (AND/NAND/OR/NOR/XOR/XNOR) gates. We supposed that the dual-rail paths have the same length, e.g., achieved by the fat-wire approach [30]. We further ignored any process variation, hence evaluating the SABL circuit under almost ideal situation, i.e., no imbalances. Note that these settings have been selected as this paper opts to show the impact of aging on the SABL structures, i.e., how aging can be exploited to ease the attacks on SABL, and how our solution (Masked SABL) can maintain the security over the device lifetime, rather than discussing the advantages and disadvantages of SABL itself in the presence of process variations.

As stated, we made use of Synopsys Hspice and MOSRA level 3 model to simulate the aging effects. As a side note, our simulations are based on a 40 nm commercial library. For the simulations, the circuit's input was kept constant during the aging phase to simulate BTI effect while `clk` was still provided by a periodic signal. Therefore, the SABL gates were switching between precharge and evaluation phases, hence the cross-coupled inverters in each SABL cell switch and simulate HCI effect. In short, these simulations cover both BTI and HCI aging mechanisms.

In order to extract dynamic power (current) signals, for each given 4-bit input to the underlying S-box, we simulated the circuit for a total of 4 clock cycles to allow SABL-cells' internal latches to gain correct complementary values. We further continued each simulation for a very long time with stable inputs in the evaluation phase (`clk` being high) to let the circuit's current and voltage settle on their steady-state values thereby emulating static-power measurements [18]. Therefore, we collected 16 dynamic power traces associated to 16 different S-box inputs, and respectively 16 static power singular values. This process has been identically repeated 8 more times after the circuit is aged for a week, i.e., a set of simulations after each week (totally 8 weeks). Note that during aging, we set the S-box input to a fixed value (all zero) and the temperature to 90° C while keeping the clock signal active, i.e., interchanging between pre-charge and evaluation phases. While the dynamic power signals have been collected at nominal temperature 21° C, the static-power measurements have been conducted at 90° C (as suggested in [12], [18]).

Figure 4(a) shows the collected static power values as well as their variance over the aging time. As expected, the amount of leakage current is reduced over time (as the transistors' threshold voltage increased); more importantly – aligned with our predictions – their diversity (resp. variance) is increased. This can potentially lead to a higher vulnerability to power analysis attacks, which we investigate in Section V. The same concept is shown by Figure 4(b), representing the variance of a part of dynamic power traces in the evaluation phase.

IV. GATE-LEVEL MASKING AS AN AGING-AWARE SOLUTION

As shown above, aging can degrade the balancedness of SABL cells. This imbalancedness originates from the unequal switching activity of the PMOS transistors of the cross-coupled inverters during the aging period (see Figure 1). In this case, we actually observe HCI effects, which – as stated in Section II-B – is one of the dominant factors among the aging mechanisms. Although several techniques

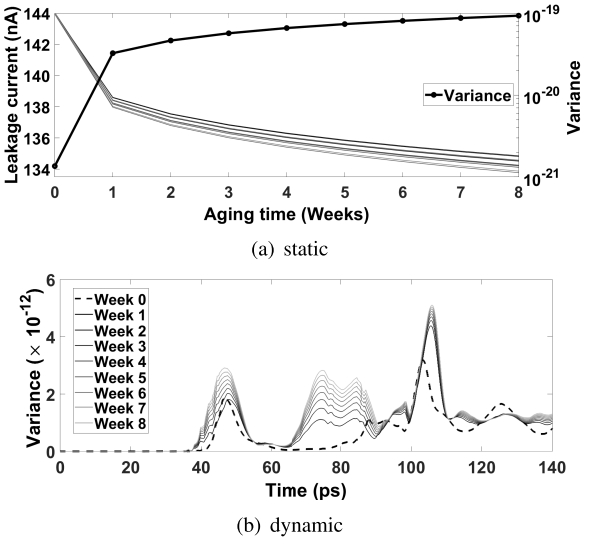


FIGURE 4. SABL S-box, result of static and dynamic power simulations over aging time. The leakage current curves shown in Fig. 4(a) are associated with 16 different S-box inputs (`0000` to `1111`).

have been proposed to mitigate the aging effects from a reliability perspective [8], [14], few studies concern the impact of aging on the circuits security [15]. Since aging is inevitable, we look for a technique to somehow force the corresponding transistors to age identically, rather than avoiding the HCI. In short, our solution, as a proactive countermeasure, tries to randomize the switching activity of the aforementioned PMOS transistors. This can mitigate the HCI's impact on information leakage originating from such an imbalancedness.

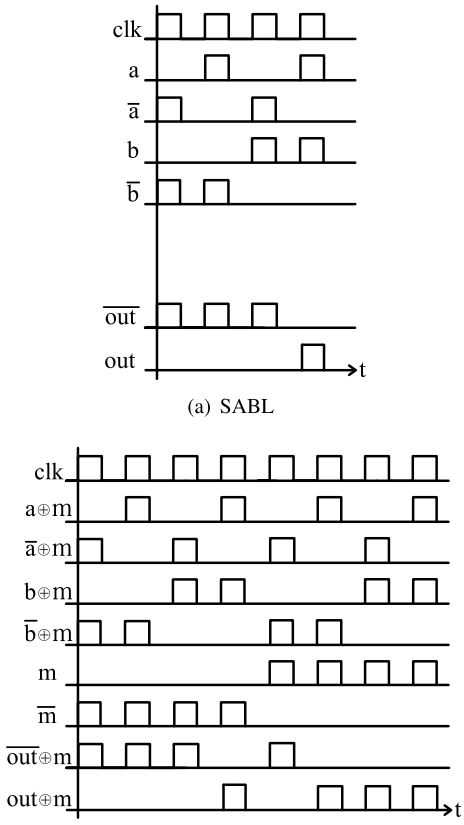
In order to achieve our goal, we borrow the concept of gate-level masking employed in Masked Dual-rail Pre-charge Logic (MDPL) [23]. We, however, first shortly review the basics of masking schemes. Based on *secret sharing*, in the simplest form of masking, a secret value $\mathtt{x}$ is represented by two shares $(\mathtt{x}_0, \mathtt{x}_1)$ in such a way that $\forall \mathtt{x}_0, \mathtt{x}_1, \mathtt{x} = \mathtt{x}_0 \oplus \mathtt{x}_1$, with $\oplus$ being the addition modulo 2 (XOR). Having only $\mathtt{x}_0$ or $\mathtt{x}_1$, no information about $\mathtt{x}$ should be revealed. Therefore, each of them should have a uniform distribution. To this end, $\mathtt{x}_0$ can be selected uniformly as random and $\mathtt{x}_1$ can be calculated as $\mathtt{x} \oplus \mathtt{x}_0$. More precisely, the primary inputs of the circuit are first masked using uniformly-distributed random numbers and at the end of the computations, the primary outputs are unmasked before being sent outside (naturally by XORing the output shares, e.g., $\mathtt{y}_0 \oplus \mathtt{y}_1$). All intermediate values of the circuit are similarly presented by two shares and all operations are performed on shared values. If implemented correctly, this avoids the leakages of the circuit to be exploitable through ordinary (first-order) SCA attacks. For more information on this topic, the interested reader is referred to [20].

The goal of MDPL is to relax the necessity of symmetric routing of dual rails [23]. Its basic idea is based on the aforementioned masking technique, but it uses masking to randomly swap the dual rails at every clock cycle. For this purpose, it uses a randomly-generated single-bit mask $\mathtt{m}$ to toggle all signals of the circuit. More precisely, instead of representing an exemplary complementary signal by $(\mathtt{x}, \overline{\mathtt{x}})$, its masked form $(\mathtt{x} \oplus \mathtt{m}, \overline{\mathtt{x}} \oplus \mathtt{m})$ is used. This holds for all complementary signals of the circuit; hence, every gate should additionally receive the complementary signal $(\mathtt{m}, \overline{\mathtt{m}})$. Note that, in contrast to an ordinary masked implementation, a single-bit mask $\mathtt{m}$ is used to mask all signals of the circuit. For simplicity, we can suppose that for $\mathtt{m} = 0$ the circuit operates as a normal dual-rail (not masked) design, and for $\mathtt{m} = 1$ all cells' input and output signals toggle their values (dual rails swapped). Note that independent of this feature, MDPL suffers from data-dependent time-of-evaluation, degrading its promised security [27], which has been corrected in the successor's design improved MDPL (iMDPL) [22]. Both use the same concept of single-bit gate-level masking, and their difference is in the design of gates to avoid early-propagation effect [27].

Here, we make use of the same concept and swap the SABL dual rails based on a random mask bit in order to equally distribute the aging effect on both rails independent of processed data. Figure 5(a) shows all possible input states and their corresponding outputs for an SABL AND/NAND cell. It can be seen that naturally only one of the outputs switches for each input value. However, considering a uniform distribution for the inputs, the switching rate of $\overline{\mathtt{out}}$ is three times more than that of $\mathtt{out}$. It means that they are differently affected by the HCI aging.

Now, consider a situation where we mask all signals of the SABL AND/NAND gate by a single-bit mask bit $\mathtt{m}$. Figure 5(b) shows the corresponding timing diagram. Suppose that the mask bit $\mathtt{m}$ is taken from a uniform distribution independent of the other signals. A single Linear Feedback Shift Register (LFSR) with e.g., 64-bit state is a resource-efficient solution to generate such a pseudo-random mask bit per clock cycle. In that case, $\mathtt{out} \oplus \mathtt{m}$ and $\overline{\mathtt{out}} \oplus \mathtt{m}$ have the same switching rate (each 4 out of 8, see Figure 5(b)). Therefore, the corresponding transistors of the cross-coupled inverters would have the same switching rate; hence, both sides of the cross-coupled inverters (corresponding to $\mathtt{out}$ and $\overline{\mathtt{out}}$) age identically from the HCI perspective. Further, as shown in Figure 5(b), the output rails are balanced in terms of duration of 0 and 1, hence balancing the BTI effect as well. This concept is our basic idea to design masked SABL to keep the balancedness thereby preventing aging-induced information leakage in SABL circuits.

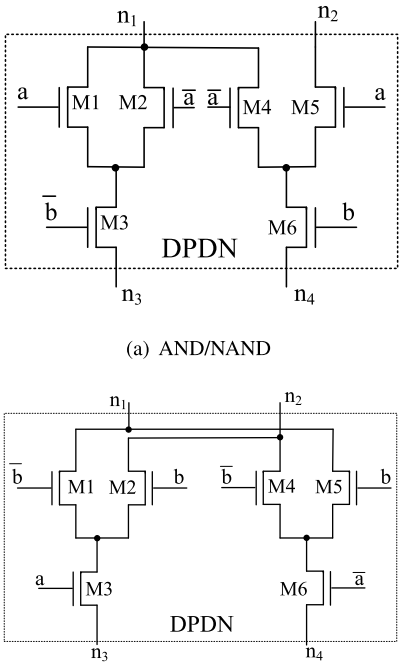
In order to design a masked SABL cell, we need to add a randomly-generated single-bit mask $\mathtt{m}$ and its complementary signal $\overline{\mathtt{m}}$ to each SABL cell. As stated above, such a single bit mask is shared between all logic cells. In other words, only a single instance of the aforementioned LFSR is sufficient for the entire circuit independent of its size. The masked SABL DPDN should work similar to that of the SABL cell for $\mathtt{m} = 0$, while it should realize the equivalent function by inverting all inputs and outputs for $\mathtt{m} = 1$. Note that, the primary inputs of the circuit should be first masked with *m* before being turned into the dual-rail and precharge form



(a) SABL

(b) Masked SABL

FIGURE 5. Timing diagram of the AND/NAND gate for all possible input values.



(a) AND/NAND

(b) XOR/XNOR

FIGURE 6. DPDN of SABL cells.

and being given to any logical cell ($s \mapsto s_m = s \oplus m$). The primary outputs should also be unmasked before being issued as output ($s_m \mapsto s = s_m \oplus m$).

As a reference, the DPDN structure of the SABL AND/NAND and XOR/XNOR gates are shown in Figure 6. Following the procedure given in [31], we need to construct enhanced DPDNs fulfilling the below given two requirements. Note that, the two other requirements indicated in Section II-A for the correctness of a DPDN are inherently fulfilled.

- For any complementary input combination, each internal node of the DPDN should be connected to either n_1 or n_2 nodes. This way, all internal nodes are discharged during the evaluation phase and charged during the precharge phase.
- The evaluation depth of the DPDN should be the same for all input combinations.

The evaluation depth is defined as the total resistance between the nodes n_1/n_2 and the circuit's common GND. Hence, the number of transistors in each route between n_1/n_2 and n_3/n_4 should be the same. If different routes have different number of transistors, we insert a path-gate in the route that has fewer transistors. A path-gate is a parallel combination of two transistors driven by a signal and its complement. Therefore, a path-gate is always "on" for complementary inputs, and it is just used to balance the resistance between different routes. Figure 7 shows the structure of DPDN of the masked SABL ANAD/NAND and XOR/XNOR gates. As an example, transistors M1, M2 as well as M8, M9 form a path-gate in masked SABL AND/NAND gate (Figure 7(a)). Note that the AND/NAND gate can be easily turned into the OR/NOR gate by swapping the complementary inputs and output signals.

V. ANALYSIS

Based on the implementation and the setup introduced in Section III, we constructed the equivalent circuit (PRESENT S-box) using our designed masked SABL cells. To this end, every SABL cell is exchanged with its masked counterpart and the complementary mask signals (m, $\overline{m}$) are connected to all cells. Naturally, we repeated all simulations with identical settings as for the SABL, explained in Section III-C. Compared to before, here we needed to conduct the simulations once for $m = 0$ and one more time for $m = 1$. Since the mask bit is supposed to be out of control of the adversary and should have a uniform distribution (essential requirements of masking schemes [17]), we took the average of every two simulations associated to $m \in \{0, 1\}$. Hence, similar to the SABL case, for each aging step (a week) we obtained 16 dynamic power signals and 16 static power values corresponding to all possible S-box inputs.

As the first analysis step, we show the variance of both static and dynamic simulation data over aging time in Figure 8, which clearly represents the benefit of our

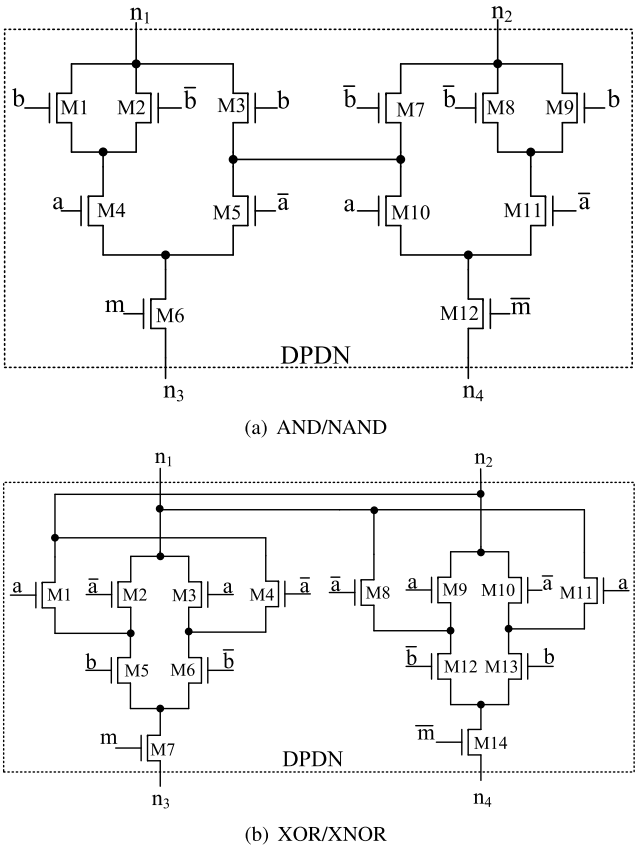


FIGURE 7. DPDN of our designed masked SABL cells.

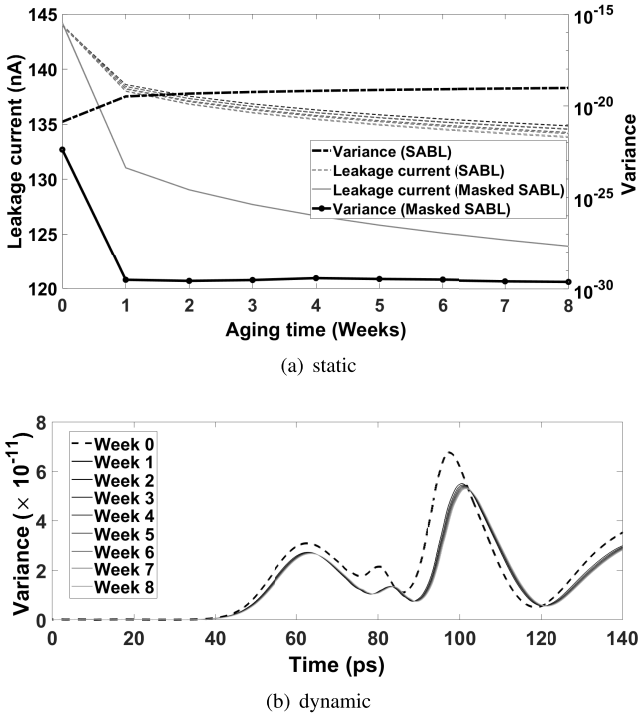


FIGURE 8. Masked SABL versus SABL S-box, result of static and dynamic power simulations over aging time. The leakage current curves shown in Fig. 8(a) are associated with 16 different S-box inputs (`0000` to `1111`). The leakage current curves for masked SABL have overlap for different S-box inputs and cannot be easily differentiated.

construction compared to the SABL in Figure 4. In short, it can be seen that – in contrast to SABL – the variance of leakages in our construction decreases when the circuit is aged. We would also like to highlight that the gray curves, shown in Figure 8(a) as the leakage current (static power) of masked SABL for all possible S-box inputs, are plotted on top of each other. They seem to be a single curve due to their similarity, but actually 16 different curves (for S-box input `0000` to `1111`) are plotted. Although variance curves already represent the benefit of our construction compared to the SABL, such a high similarity between the curves is not observed in those plotted in Figure 4.

A. LEAKAGE ANALYSIS

In contrast to simulation, experimental SCA measurements are affected by noise originating from the measurement setup and environmental parameters. Hence, the aim of a proper SCA evaluation in the simulation domain is to examine the success of corresponding attacks over the noise level. Considering a Gaussian noise, Information-Theoretic (IT) analysis [26] evaluates the amount of information in SCA leakages associated with processed data. In short, it estimates mutual information utilizing conditional entropy as

$$\mathrm{I}(S; L) = \mathrm{H}[S] - \mathrm{H}[S|L],$$

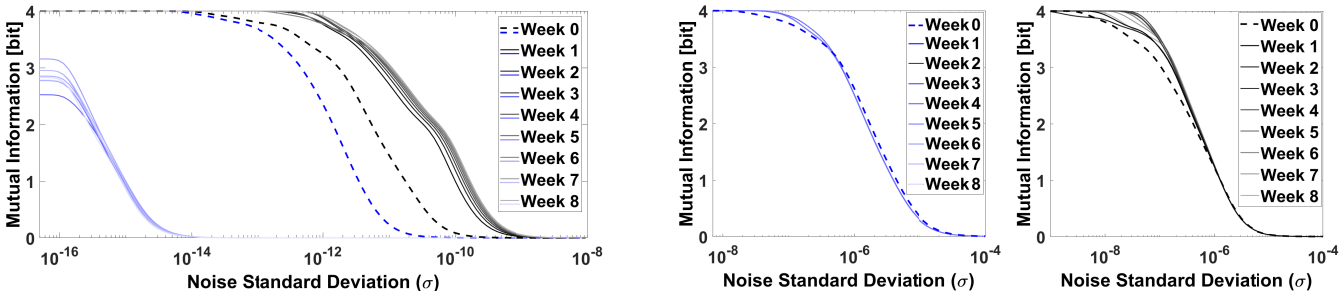
where L denotes the SCA leakages and S the selected intermediate value (the S-box input in our case study). The conditional entropy can be estimated by means of integral over l as

$$\mathrm{H}[S|L] = -\sum_{s} \Pr[s] \int \Pr[l|s] \cdot \log_2 \Pr[s|l]\, dl.$$

This analysis, which is suitable to compare different countermeasures under similar settings, extracts a curve for mutual information over noise standard deviation. It identifies the necessary noise level to entirely hide the information leakage. The lower the required noise, the higher is the robustness as the leakage can more easily (with lower noise) be hidden. It is worth mentioning that such a technique has been considered as a valid analysis scheme for DPA-resistant logic styles (see for example [16], [25]).

We performed this analysis on static power simulation data which we have collected from both original and masked SABL circuits for all aging times. The corresponding result, shown in Figure 9(a) confirms the ability of our construction to better hide the information leakage when the device is aged. The SABL circuit needs more noise over aging time, while this is opposite in our masked SABL variant. Note that since we considered the SCA leakages associated to the input of an S-box instance, the maximum of the extracted mutual information curves is 4, as the S-box has a 4-bit input.

We repeated the same procedure for all sample points of dynamic power simulation data sets. This way, a mutual information curve for each sample point and each aging time



(a) static (b) dynamic

FIGURE 9. Mutual information curves for both static and dynamic power based on the S-box input, for both masked SABL (blue) and SABL (black).

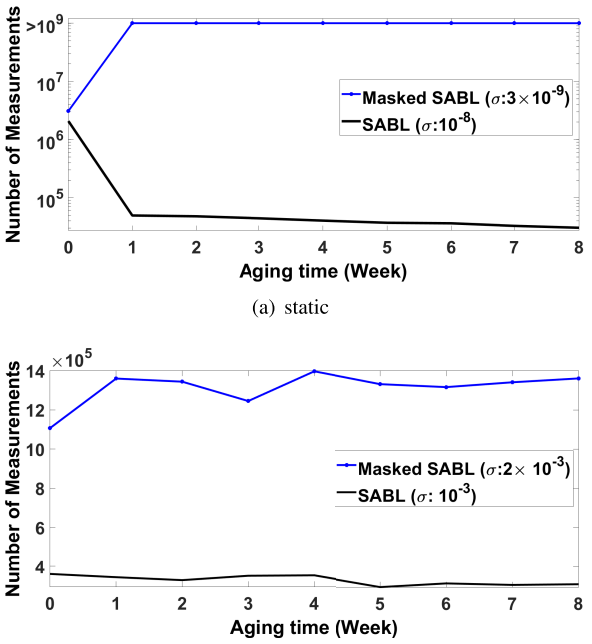
is extracted. To be able to compare the results, for each given noise standard deviation, we need to observe the maximum of mutual information for all sample points. This had led to the results shown in Figure 9(b). The benefit is not as significant as that for static power measurements. However, as the most important fact, in contrast to the SABL circuit, the leakage of the masked SABL design (slightly) decreases over aging time.

B. ATTACKS

In addition to the IT analysis which presents the minimum amount of noise to hide the remaining leakages, we conducted state-of-the-art attacks to obtain an overview on the number of measurements required to exploit the leakages. To this end, we apply Moment-Correlating DPA (MC-DPA) [19], which – compared to the other DPA attacks – relaxes the necessity of having a hypothetical power model. In particular, we conducted collision MC-DPA, which examines the exploitability of leakages. It divides the traces into two equal-size groups: one to extract the model (through average in case of first-order MC-DPA), and the other one to conduct the attack based on the extracted model. If successful, MC-DPA in general recovers the linear difference (XOR) of secret keys associated to the two aforesaid groups of traces.

Since the simulation data are noise-free, we need to artificially add Gaussian noise to the collected simulation data set to emulate an experimental situation. As stated, for each circuit and for each aging time, we have a vector of 16 elements as noise-free static power values associated to the S-box input values (this holds for each sample point in case of dynamic power traces). Therefore, for the given noise standard deviation σ, by gathering the noisy values, we obtain a set of let say n samples (either for static power or for each sample point of dynamic power traces). More precisely, a 16-element vector is repeated a required number of times to reach the desired size n. Afterwards, it is added with n noise samples, taken from a Gaussian distribution with standard deviation σ, to form a vector of n noisy measurements.

By gradually increasing n, and conducting the MC-DPA attack following the explanation above, we obtained the minimum number of measurements leading to a successful attack. Since this conclusion depends on the Gaussian



(a) static

(b) dynamic

FIGURE 10. Minimum required number of measurements for successful MC-DPA attacks.

(but randomly) added noise, we repeated this process 100 times and took average of minimum number of required measurements. Repeating the same procedure on all data sets (static, dynamic, and all aging times) led to the curves presented in Figure 10. Aligned with the IT-based analysis, equivalent attacks on SABL circuit need less traces when the device is aged. In contrast, the attacks on our masked SABL construction become harder over the device lifetime.

It might be seen questionable that we could perform successful attacks on an SABL circuit without considering imbalances originating from process variations. Note that the parasitic elements cause DPDN to switch (very slightly) differently for various inputs. Therefore, considering no noise (or very little noise) the traces captured by Hspice simulations can show the data dependency of the traces, and hence the SABL circuit could be successfully attacked. As shown in [16] any DPA-resistant logic style (including SABL) can be attacked given very low (or zero) amount of noise.

C. OVERHEAD

We would also like to point out that the application of our masked SABL cells leads to a higher overhead compared to the original ones. As the most obvious fact, the dual-rail mask signal ($\mathtt{m}, \overline{\mathtt{m}}$) should be routed to all cells of the circuit. This slightly increases the complexity of the design process, although the facility of routing clock signal can be re-used for this purpose. Further, 6 and 8 more NMOS transistors are used in AND/NAND and XOR/XNOR cells compared to SABL. This makes the corresponding DPDNs larger which for sure have some impact on the power and delay of the circuit.

We assessed this fact using the above-explained case study, i.e., the PRESENT S-box. In total, the masked SABL S-box requires 112 more NMOS transistors. This leads to around 18.7% larger area compared to the circuit constructed using SABL cells, based on the used 40 nm commercial library. Note that both circuits have exact the same topology, while being only different in the type of the instantiated gates. Our investigations show that their amount of power consumption (averaged over all possible input values) are very similar while our masked SABL circuit exhibits around 13.8% higher delay. For the delay, we considered the average time the circuit requires to evaluate the S-box output for all possible input values. Table 1 summarizes these results. The takeaway point from all these observations is that employing our-designed masked SABL cells can maintain the security of the circuit over its lifetime, with an acceptable overhead.

TABLE 1. Overhead of masked SABL versus SABL, based on an implementation of the PRESENT S-box.

Overhead	Masked SABL vs SABL
Area	+ 18.7%
Power	+ 1.07%
Delay	+ 13.8%

VI. CONCLUSION

In this paper, we focused on DPA-resistant dual-rail pre-charge logic styles, in particular on SABL. Such countermeasures are supposed to harden power analysis attacks by means of equalizing the amount of power consumption independent of the circuit's activity. We showed that DPA resistance of SABL circuits can be affected by the aging-induced change of the device specifications over time, which results in imbalances in dual rails and in turn increases the vulnerability of the circuit to key-recovery SCA attacks. We proposed to integrate a gate-level masking into the SABL cells' structure thereby randomly swapping the content of dual rails. This avoids the transistors associated to a certain rail of a gate to switch more than the others, hence balancing the effect of aging on both rails independent of the gate's input. The analysis results based on both dynamic and static power profiles confirm the efficacy of our proposed technique in maintaining the security of the corresponding circuits to power analysis attacks over the device lifetime.

ACKNOWLEDGMENT

This work was supported in part by the Deutsche Forschungsgemeinschaft (DFG) through the Germany's Excellence Strategy under Grant EXC 2092 CASA-390781972, in part by the Project "Aged but Fit: Long Lasting Security for Trusted Platforms" under Grant 418658052, and in part by the National Science Foundation, Faculty Early Career Development (CAREER) Award through the Project "Investigating the Impact of Device Aging on the Security of Cryptographic Chips" under Grant NSF CNS-1943224. A preliminary version of this paper was presented at the 2021 Asia and South Pacific Design Automation Conference [4].

REFERENCES

[1] M. A. Alam, H. Kufluoglu, D. Varghese, and S. Mahapatra, "A comprehensive model for PMOS NBTI degradation: Recent progress," *Microelectron. Rel.*, vol. 47, no. 6, pp. 853–862, Jun. 2007.

[2] M. T. H. Anik, J. Danger, S. Guilley, and N. Karimi, "Detecting failures and attacks via digital sensors," *IEEE Trans. Computer-Aided Design Integr. Circuits Syst.*, vol. 40, no. 7, pp. 1315–1326, Jul. 2021.

[3] M. T. H. Anik, S. Guilley, J.-L. Danger, and N. Karimi, "On the effect of aging on digital sensors," in *Proc. 33rd Int. Conf. VLSI Design 19th Int. Conf. Embedded Syst. (VLSID)*, Jan. 2020, pp. 189–194.

[4] 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. 26th Asia South Pacific Design Autom. Conf.*, Jan. 2021, pp. 414–420.

[5] D. Bellizia, S. Bongiovanni, M. Olivieri, and G. Scotti, "SC-DDPL: A novel standard-cell based approach for counteracting power analysis attacks in the presence of unbalanced routing," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 67, no. 7, pp. 2317–2330, Jul. 2020.

[6] D. Bellizia, G. Scotti, and A. Trifiletti, "TEL logic style as a countermeasure against side-channel attacks: Secure cells library in 65nm CMOS and experimental results," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 65, no. 11, pp. 3874–3884, Nov. 2018.

[7] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, and C. Vikkelsoe, "PRESENT: An ultra-lightweight block cipher," in *Cryptographic Hardware and Embedded Systems* (Lecture Notes in Computer Science), vol. 4727. Berlin, Germany: Springer, 2007, pp. 450–466.

[8] A. Gebregiorgis, M. Ebrahimi, S. Kiamehr, F. Oboril, S. Hamdioui, and M. B. Tahoori, "Aging mitigation in memory arrays using self-controlled bit-flipping technique," in *Proc. 20th Asia South Pacific Design Autom. Conf.*, Jan. 2015, pp. 231–236.

[9] J. Giorgetti, G. Scotti, A. Simonetti, and A. Trifiletti, "Analysis of data dependence of leakage current in CMOS cryptographic hardware," in *Proc. 17th Great Lakes Symp. Great Lakes Symp. VLSI (GLSVLSI)*, 2007, pp. 78–83.

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

[11] N. Karimi, J. Danger, F. Lozach, and S. Guilley, "Predictive aging of reliability of two delay PUFs," in *Security, Privacy, and Applied Cryptography Engineering* (Lecture Notes in Computer Science), vol. 10076. Hyderabad, India: Springer, 2016, pp. 213–232.

[12] N. Karimi, T. Moos, and A. Moradi, "Exploring the effect of device aging on static power analysis attacks," in *Proc. TCHES*, vol. 2019, no. 3, 2019, pp. 233–256.

[13] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Advances in Cryptology*, vol. 1666. Berlin, Germany: Springer, 1999, pp. 388–397.

[14] D. Kraak, I. Agbo, M. Taouil, S. Hamdioui, P. Weckx, S. Cosemans, and F. Catthoor, "Hardware-based aging mitigation scheme for memory address decoder," in *Proc. IEEE Eur. Test Symp. (ETS)*, May 2019, pp. 1–6.

[15] D. Kraak, M. Taouil, S. Hamdioui, P. Weckx, F. Catthoor, A. Chatterjee, A. Singh, H.-J. Wunderlich, and N. Karimi, "Device aging: A reliability and security concern," in *Proc. IEEE 23rd Eur. Test Symp. (ETS)*, May 2018, pp. 1–10.

[16] F. Macé, F.-X. Standaert, and J.-J. Quisquater, "Information theoretic evaluation of side-channel resistant logic styles," in *Cryptographic Hardware and Embedded Systems (CHES)*. Berlin, Germany: Springer, 2007, pp. 427–442.

[17] S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks: Revealing the Secrets of Smart Cards*. New York, NY, USA: Springer, Dec. 2006.
[18] A. Moradi, "Side-channel leakage through static power–should we care about in practice," in *Cryptographic Hardware and Embedded Systems—CHES* (Lecture Notes in Computer Science), vol. 8731. Busan, South Korea: Springer, 2014, pp. 562–579.
[19] A. Moradi and F.-X. Standaert, "Moments-correlating DPA," in *Proc. ACM Workshop Theory Implement. Secur.*, Oct. 2016, pp. 5–15.
[20] S. Nikova, V. Rijmen, and M. Schläffer, "Secure hardware implementation of nonlinear functions in the presence of glitches," *J. Cryptol.*, vol. 24, no. 2, pp. 292–321, Apr. 2011.
[21] F. Oboril and M. B. Tahoori, "ExtraTime: Modeling and analysis of wearout due to transistor aging at microarchitecture-level," in *Proc. IEEE/IFIP Int. Conf. Dependable Syst. Netw. (DSN)*, Jun. 2012, pp. 1–12.
[22] T. Popp, M. Kirschbaum, T. Zefferer, and S. Mangard, "Evaluation of the masked logic style MDPL on a prototype chip," in *Cryptographic Hardware and Embedded Systems—CHES* (Lecture Notes in Computer Science), vol. 4727. Vienna, Austria: Springer, Sep. 2007, pp. 81–94.
[23] T. Popp and S. Mangard, "Masked dual-rail pre-charge logic: DPA-resistance without routing constraints," in *Cryptographic Hardware and Embedded Systems—CHES* (Lecture Notes in Computer Science), vol. 3659. Scotland, U.K.: Springer, Sep. 2005, pp. 172–186.
[24] M. T. Rahman, D. Forte, J. Fahrny, and M. Tehranipoor, "ARO-PUF: An aging-resistant ring oscillator PUF design," in *Proc. Design, Autom. Test Eur. Conf. Exhib. (DATE)*, 2014, pp. 1–6.
[25] M. Renauld, D. Kamel, F.-X. Standaert, and D. Flandre, "Information theoretic and security analysis of a 65-nanometer DDSLL AES S-box," in *Cryptographic Hardware and Embedded Systems—CHES* (Lecture Notes in Computer Science), vol. 6917, B. Preneel and T. Takagi, Eds. Nara, Japan: Springer, 2011, pp. 223–239.
[26] F.-X. Standaert, T. Malkin, and M. Yung, "A unified framework for the analysis of side-channel key recovery attacks," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 5479, A. Joux, Ed. Springer, Apr. 2009, pp. 443–461.
[27] D. Suzuki and M. Saeki, "Security evaluation of DPA countermeasures using dual-rail pre-charge logic style," in *Cryptographic Hardware and Embedded Systems—CHES* (Lecture Notes in Computer Science), vol. 4249. Yokohama, Japan: Springer, 2006, pp. 255–269.
[28] K. Tiri, M. Akmal, and I. Verbauwhede, "A dynamic and differential CMOS logic with signal independent power consumption to withstand differential power analysis on smart cards," in *Proc. ESSCIRC*, Sep. 2002, pp. 403–406.
[29] K. Tiri and I. Verbauwhede, "A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation," in *Proc. Design, Autom. Test Eur. Conf. Exhib.*, Feb. 2004, pp. 246–251.
[30] K. Tiri and I. Verbauwhede, "Place and route for secure standard cell design," in *Smart Card Research and Advanced Applications VI* (IFIP International Federation for Information Processing), vol. 153. Boston, MA, USA: Springer, 2004, pp. 143–158.
[31] K. Tiri and I. Verbauwhede, "Design method for constant power consumption of differential logic circuits," in *Proc. Design, Autom. Test Eur.*, Mar. 2005, pp. 628–633.
[32] S. Zafar, Y. Kim, V. Narayanan, C. Cabral, V. Paruchuri, B. Doris, J. Stathis, A. Callegari, and M. Chudzik, "A comparative study of NBTI and PBTI (charge trapping) in SiO_2/HfO_2 stacks with FUSI, TiN, Re gates," in *Symp. VLSI Technol., Dig. Tech. Papers.*, Jun. 2006, pp. 23–25.

BIJAN FADAEINIA received the B.Sc. degree in electrical engineering from the University of Tabriz, Iran, in 2001, and the M.Sc. degree in electrical engineering from the Iran University of Science and Technology, Iran, in 2004. He is currently pursuing the Ph.D. degree with the Chair for Security Engineering, Horst-Görtz Institute for IT-Security, Ruhr-Universität Bochum, Germany. From 2004 to 2019, he worked as a Lecturer with the Department of Electrical Engineering, Islamic Azad University of Hamadan, Iran. He is also a Scientific Research Assistant with the Chair for Security Engineering, Horst-Görtz Institute for IT-Security, Ruhr-Universität Bochum. His research interests include physical security of embedded devices and hardware-based countermeasures.

MD TOUFIQ HASAN ANIK (Graduate Student Member, IEEE) received the B.S. degree in electrical and electronics engineering from Brac University, Bangladesh, in 2016. He is currently pursuing the Ph.D. degree in computer engineering with the University of Maryland at Baltimore County (UMBC). He worked as a Security Researcher Intern at Intel, during summer 2020. He has been working as a Computer Architecture Graduate Intern at Intel, since summer 2021. He conducts research in the SECure, REliable, and Trusted Systems (SECRETS) Research Laboratory, UMBC. His research interests include hardware security, power analysis attacks and countermeasures, sensor-assisted secure, and reliable design.

NAGHMEH KARIMI (Member, IEEE) 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 with Yale University, USA, from 2007 to 2009, and a Postdoctoral Researcher with Duke University, USA, from 2011 to 2012. She was a Visiting Assistant Professor with New York University and Rutgers University, from 2012 to 2016. In 2017, she joined the University of Maryland at Baltimore County, as an Assistant Professor, where she leads the SECure, REliable and Trusted Systems (SECRETS) Research Laboratory. She has published three book chapters and authored/coauthored more than 60 articles in refereed conference proceedings and journal manuscripts. Her current research interests include hardware security, VLSI testing, design-for-trust, design-for-testability, and design-for-reliability. She was a recipient of the National Science Foundation CAREER Award, in 2020. She also serves as an Associate Editor for the *Journal of Electronic Testing: Theory and Applications (JETTA)* (Springer). She has been the Corresponding Guest Editor of the IEEE JOURNAL ON EMERGING AND SELECTED TOPICS IN CIRCUITS AND SYSTEMS Special Issue on "Hardware security in emerging technologies."

AMIR MORADI received the M.Sc. and Ph.D. degrees in computer engineering from the Sharif University of Technology, Tehran, Iran, in 2004 and 2008, respectively, and the Habilitation degree, in 2016. From 2008 to 2015, he worked as a Postdoctoral Researcher with the Chair for Embedded Security, Ruhr Universität Bochum, Germany. In 2016, he joined the Faculty of Electrical Engineering and Information Technology, Ruhr Universität Bochum, where he is currently a Professor. He has published over 120 peer-reviewed journal articles and conference papers, in both destructive and constructive aspects of side-channel analysis. His current research interests include physical security of embedded systems, passive and active physical attacks, and the corresponding countermeasures. He served as a program committee member (and the chair) of several security- and cryptography-related conferences and workshops.