Toward Security Closure in the Face of Reliability Effects

ICCAD Special Session Paper

Jens Lienig
TU Dresden
jens@ieee.org

Susann Rothe
TU Dresden
susann.rothe@tu-dresden.de

Matthias Thiele
TU Dresden
matthias.thiele@tu-dresden.de

Nikhil Rangarajan
NYU Abu Dhabi
nikhil.rangarajan@nyu.edu

Mohammed Ashraf
NYU Abu Dhabi
ma199@nyu.edu

Mohammed Nabeel
NYU Abu Dhabi
mtn2@nyu.edu

Hussam Amrouch
University of Stuttgart
amrouch@iti.uni-stuttgart.de

Ozgur Sinanoglu
NYU Abu Dhabi
ozgursin@nyu.edu

Johann Knechtel
NYU Abu Dhabi
johann@nyu.edu

***Abstract*—The reliable operation of ICs is subject to physical effects like electromigration, thermal and stress migration, negative bias temperature instability, hot-carrier injection, etc. While these effects have been studied thoroughly for IC design, threats of their subtle exploitation are not captured well yet. In this paper, we open up a path for *security closure of physical layouts* in the face of reliability effects. Toward that end, we first review migration effects in interconnects and aging effects in transistors, along with established and emerging means for handling these effects during IC design. Next, we study security threats arising from these effects; in particular, we cover migration effects-based, disruptive Trojans and aging-exacerbated side-channel leakage. Finally, we outline corresponding strategies for security closure of physical layouts, along with an outline for CAD frameworks.**

***Index Terms*—Hardware Security, Physical Layouts, Electromigration, CAD, Trojans, Aging, Side-Channel Attacks**

I. Introduction

Reliability of ICs represents an ever-more increasing challenge, due to continuous downscaling of structural dimensions and increasing demand for performance. Physical effects like electromigration or negative bias temperature instability play key roles for reliability [1]–[3]. Thus, handling these effects during IC design is paramount, especially for advanced nodes [4]–[6].

At the same time, there is the threat of stealthy attacks that exploit reliability effects. For example, some malicious modification of the power stripes (during mask generation or manufacturing) can lead to migration-induced failures, potentially rendering the whole IC inoperable [7]. However, prior art has largely overlooked this challenge, mainly because threats arising from reliability effects are not well known to the security community, whereas the circuit and CAD communities often lack the awareness of security threats.

In this paper, thus, we open up a path for *security closure of physical layouts* in the face of reliability effects.[1] Toward that end, cross-disciplinary team efforts are required, driven by security researchers and practitioners, physical-design engineers, and CAD experts. As demonstrated throughout this paper, the first tasks are to establish a shared, detailed understanding for:

1) reliability effects of concern, along with their layout-level workings (Sec. II);
2) evaluation, mitigation strategies for the effects' workings, tailored for CAD flow integration (Sec. III);
3) security threats arising for/exacerbated by the effects' workings (Sec. IV).

After building such foundation, the follow-up tasks are to:

4) derive strategies for security closure of physical layouts against the threats of concern (Sec. V-A);
5) within CAD flows, implement sign-off-grade means for assessment and mitigation of the threats of concern, following the derived strategies (Sec. V-B).[2]

II. Reliability Effects

A. Migration Effects in Interconnects

It is commonly differentiated between three types of material transport in metallic connectivity architectures that can significantly impact circuit reliability: electromigration (EM), thermal migration (TM), and stress migration (SM). Although we introduce these types of migration separately, it is important to point out that they are in fact closely coupled processes, as summarized in the final Subsection II-A4.

1) Electromigration (EM): Current flow through a conductor produces two forces, which act on the individual metal ions in the conductor (Fig. 1). If the resulting force in the direction of the electron wind exceeds a given trigger known as the activation energy E_a, a directed migration process starts.

EM failures in modern chip manufacturing processes are mostly due to *voids*. They result from the building up of tensile stress with two stages of EM degradation [9]: In the *void nucleation phase*, the tensile stress increases over time

[1] This paper is part of the special session *Security Closure of Physical Layouts* at ICCAD'21. We invite the reader to also see the session's vision paper [8] for a broader context of security closure.

[2] Contributions for this task are beyond the scope of this paper. We focus on the other tasks at hand, and outline the need for that final task.

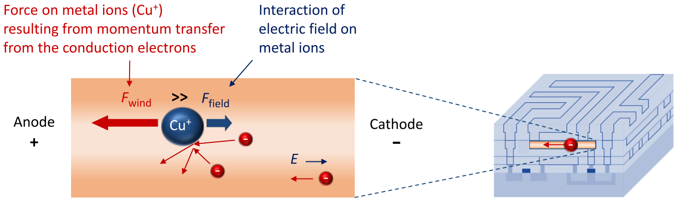
Force on metal ions (Cu+) resulting from momentum transfer from the conduction electrons
Interaction of electric field on metal ions
F_{wind} >> F_{field}
Anode
+
Cu+
Cathode
−
E

Fig. 1. Two forces act on metal ions that make up the lattice of the interconnect material [1]. Electromigration is the result of the dominant force, i.e., the momentum transfer from the electrons that move in the electric field.

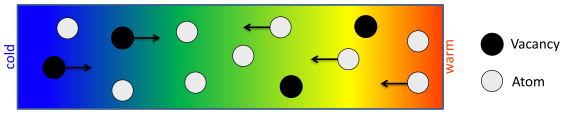

Fig. 2. Thermal migration is expressed by atomic and vacancy movement. It consists of mass transport from one local region to another, much like EM, with the difference that TM is driven by a thermal gradient rather than an electrical potential gradient [1].

but no void has nucleated. When the stress reaches a critical threshold, the void nucleates and the *void growth phase* begins.

I.A. Blech showed in [10] that a wiring segment is not susceptible to electromigration if the product of the segment's current density j and the segment's length L is less than a process-technology-dependent threshold value $(jL)_{Blech}$. The critical product $(jL)_{Blech}$ is often called the "Blech immortality condition" or "Blech effect."

Besides using current density j as the decisive parameter for describing the EM risk in IC interconnect (the well-known Black's model [11]), EM-induced mechanical stress is increasingly applied for this purpose (the so-called "Korhonen model" [12]).[3] Here, the hydrostatic stress σ arising under the influence of EM is used to characterize EM risks and guide mitigation measures. For example, a void is said to nucleate once the hydrostatic stress exceeds a predefined threshold value $\sigma_{threshold}$.

2) Thermal Migration (TM): Sometimes also referred to as *thermomigration*, TM is produced by temperature gradients. Atoms in regions of higher temperature have a greater probability of dislocation than in colder regions due to their temperature-related activation. This causes a larger number of atoms diffusing from regions of higher temperature to regions of lower temperature than atoms in the opposite direction. The result is net diffusion (mass transport) in the direction of the negative temperature gradients (Fig. 2).

3) Stress Migration (SM): Also referred to as *stress voiding* or *stress induced voiding (SIV)*, SM is atomic diffusion that causes a balancing of mechanical stress. There is a net atomic flow into regions where tensile forces are acting, whereas metal atoms flow out of regions under compressive stress. Similar to thermal migration, this leads to diffusion in the direction of the negative mechanical tension gradient (Fig. 3). As a result, the vacancy concentration is balanced to match the mechanical tension.

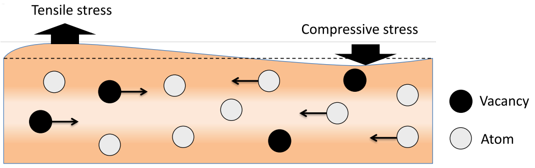

Fig. 3. Stress migration is the result of a mechanical stress gradient, either from external forces or from internal processes, such as electromigration or thermal expansion [1]. Voids form as a consequence of vacancy migration driven by the hydrostatic stress gradient.

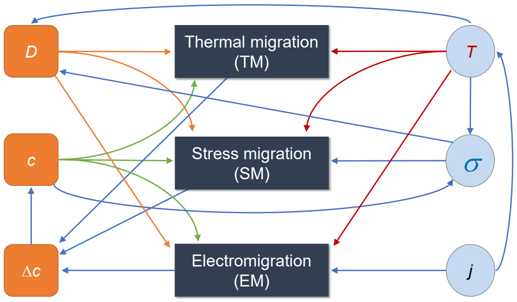

Fig. 4. Interaction between TM, SM, and EM through their driving forces temperature (T), mechanical/hydrostatic stress (σ) and current density (j) [5]. The related migration parameters, i.e., diffusion coefficient (D), concentration (c) and concentration change ($\triangle c$) are also shown.

The main causes for mechanical stress as the driving force behind SM in metal wires are thermal expansion, electromigration, and deformation through packaging.

4) Mutual Interaction: Combining various (counter-acting) migration processes can produce an equilibrium state. For example, the equilibrium between EM and SM results in the "Blech effect."

Obviously, EM, TM, and SM are closely coupled processes as their driving forces are linked with each other and with the resultant migration change, as visualized in Fig. 4 [5]. For instance, current density raises the temperature through Joule heating, and temperature change modifies mechanical stress through differences in expansion coefficients. Another example of interactions between temperature and EM is temperature-induced EM in modern FinFETs. Here, self-heating is more serious as compared to other planar transistors because of the complex geometry and missing heat paths down to the bulk. This requires complex self-heating models and design considerations, such as presented in [13].

We refer the reader to the literature, such as [1, Sec. 2.5], for further elaboration on the mutual interactions.

B. Aging Effects in Transistors

1) Fundamentals of Aging Effects: During the operation of a MOSFET transistor, activation energy provided by applied vertical and horizontal electrical fields leads to different types of defects. Those defects are undesired charges that are caused by interface traps (i.e., broken Si-H bonds at the interfacial layer) and by oxide traps (i.e., when charge carriers are tunnelled through the SiO_2 layer and then get captured by the available oxide vacancies inside the dielectric) [14]. Figure 5

[3] While Black's model calculates the reliability due to EM of a single wire segment, the Korhonen model and its subsequent extensions, e.g. by Chatterjee *et al.* [9], track the material flow in all branches of a net located within one layer of metallization.

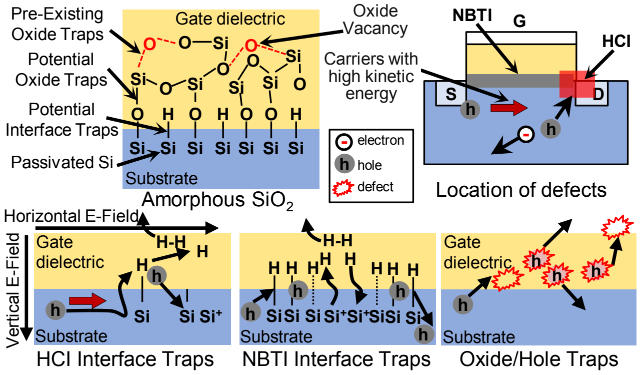

Fig. 5. Overview of the different types of defects (oxide traps and interface traps) that can be generated within a MOSFET transistor during its operation. The main underlying mechanisms are Bias Temperature Instability (BTI) and Hot-Carrier Injection (HCI). Derived from [17].

illustrates how interface and oxide traps can be induced by aging mechanisms.

Over time, such generated defects (i.e., interface and oxide traps) accumulate inside the transistor and degrade its performance. *Positive/Negative Bias Temperature Instability (PBTI/NBTI)* and *Hot-Carrier Injection (HCI)* are the most prominent aging phenomena that are responsible for stimulating the underlying defect generation mechanisms. They have the potential to remarkably degrade the key electrical characteristics of pMOS and nMOS transistors, such as threshold voltage (V_{th}), as illustrated in Fig. 6 [2], as well as carrier mobility (μ) and sub-threshold slope (SS) [15].

An increase in V_{th} along with a decrease in μ and SS directly impact the ON and OFF currents of MOSFETs. On the one hand, the ON current of transistor decreases, which degrades the transistor switching speed. As a result, aging over time prolongs the delay of the critical paths of circuits. Consequently, errors caused by timing violations start to appear because of unsustainable clock frequencies, leading to unreliable operation [2], [16]. On the other hand, the OFF current of transistor increases, which reduces the static power of circuits. Note that reductions in the ON current result in less dynamic power. All in all, aged circuits exhibit larger delays as well as smaller static and dynamic power.

To overcome aging-induced delay increases and ensure proper functionality for the circuit, the so-called *timing guardbands* need to be carefully estimated and then included on top of the maximum clock period. While overestimating guardbands leads to efficiency losses, underestimating guardbands leads to unreliable operation during the circuit's lifetime.

2) Intrinsic Aging Stimuli: BTI occurs due to the induced stress by the vertical field and it results in interface traps as well as oxide traps. HCI occurs when both vertical and lateral electric fields are applied in which carriers gain sufficient kinetic energy to become "hot" and hence injected inside the interfacial layer leading to interface traps. Over time, generated defects (i.e., interface and oxide traps) accumulate and manifest themselves as an increase in V_{th} along with a decrease in μ. As can be noticed from Eq. 1, a reduction in the carrier mobility (μ) and/or an increase in the transistor threshold voltage (ΔV_{th}), directly results in lower ON current. This, in turn, reduces the switching speed of transistors and hence increases the propagation delay of transistor (T_{delay}).

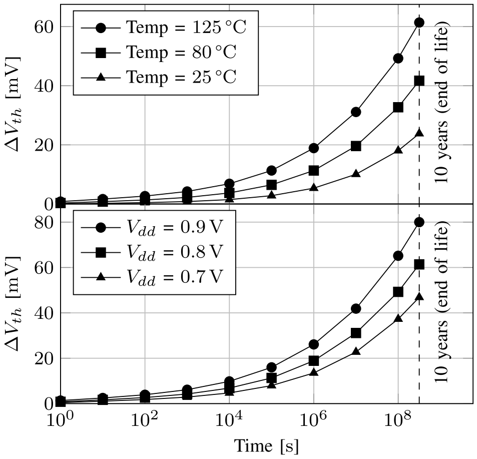

Fig. 6. Impact of temperature and voltage on stimulation aging-induced degradation (i.e., transistor threshold voltage ΔV_{th}). Analysis is done for pMOS-type transistor in an FinFET technology node. Derived from [2].

Timing violations may occur if the included timing guardband (t_{GB}) is not sufficient, as shown in Eq. 2 [2]. As mentioned earlier, such a guardband directly results in a performance loss because the circuit will be clocked at lower frequency than its maximum potential. Therefore, designers aim at estimating timing guardband to be close to edge, to minimize the induced performance and efficiency losses [18].

$$t_D \propto \frac{1}{I_{ON}} \; ; \qquad I_{ON} \approx \frac{\mu}{2} \cdot (V_{dd} - V_{th} - \Delta V_{th})^2 \qquad (1)$$

$$t_{CP} = \sum_{i \in CP} t_{D_i} \; ; \; t_{CP} \le t_{clock} \Rightarrow \textit{no timing errors} \checkmark \qquad (2)$$
$$t_{clock}(Aging) = t_{CP}(noAging) + t_{GB}$$
$$f_{clock}(Aging) < f_{clock}(noAging) \Rightarrow \textit{performance loss} \,!$$

where t_D, I_{ON}, t_{CP}, and t_{clock} refer to the transistor switching delay, transistor ON current, critical path delay, and clock period, respectively.

3) Systematic Aging Stimuli: Operating voltage and temperature (see Fig. 6) as well as duty cycle (i.e., how often the transistor is ON) determine the amount of induced degradations. In practice, the end-user has a large degree of control to aging stimuli (i.e., voltage, temperature, and duty cycle). The workload running on top of the circuit determines the induced activities and hence the duty cycles that transistors exhibit over time. The operating voltage can often be controlled by the operating system, to boost the performance when it is needed. Similarly, the operating system can often determine the amount of cooling (e.g., fan speed) and hence the chip's temperature.

III. Assessment and Mitigation of Reliability Effects During Physical Design

A. Assessing Migration Robustness

1) State-of-the-Art EM Sign-Off Process: The main reason for migration-induced chip failure in well-established semiconductor technologies is EM. Therefore, in state-of-the-art design flows, an EM verification step is performed after layout synthesis. Nets that are at danger of suffering EM-induced failure are usually modified, e.g., width-adjusted. Furthermore, improved EM robustness can be achieved by limiting current density or wire length. This strategy aims at "immortal" wires exploiting SM as a counteracting force to EM and, thus, the "Blech effect" (Sec. II-A1) [10].

A decreased current density may be accomplished by lower currents, increased wire widths and redundant vias. Wire length can be reduced by introducing layer changes, as the metal liners act as diffusion barriers blocking metal atom migration [19]. For an extensive study on the effectiveness of those measures as well as on their demand of routing resources, please refer to [4].

Currently, EM verification focuses on wires carrying direct currents (DC), such as power distribution networks. Signal lines are less susceptible to EM-induced failure because they experience a certain self-healing effect due to the alternating current (AC) [20].

2) Current Density Verification: EM sign-off tools widely used in industry, like Cadence Spectre APS EMIR [21] and ANSYS RedHawk [22], are able to verify a layout for its EM robustness, and detect potential EM hotspots that have to be corrected. The EM analysis is based on current density constraints provided by the foundry. Those tools are using a Black/Blech-based approach (Sec. II-A1) to estimate the danger of EM-induced damage in the wires by considering currents and net topology. The analysis can be coupled to the circuit's temperature characteristics as high temperatures accelerate metal migration and thus influence wire degradation.

For a more accurate simulation of current density distribution in specific layout structures, finite element analysis (FEA) can be employed. This is especially useful for comparing various topologies regarding their EM susceptibility and, thus, developing design guidelines for EM-robust layout synthesis. Moreover, FEA is often used as a reference to assess the accuracy of other EM verification methods. Yet, FEA is time consuming and thus not suited for full-chip EM analysis [23].

3) Emerging Verification Approaches: The Black/Blech-based current density verification is increasingly considered as insufficient for evaluating migration robustness in advanced technology nodes. This method lacks the required precision (and thus depends upon high safety margins) and can merely capture a limited problem complexity [20]. Therefore, novel physics-based approaches are developed for migration robustness assessment using the Korhonen model [12]. In contrast to the current density-based methods, wire degradation assessment is derived here from the occurring hydrostatic stress.

Recent academic tools [24]–[26] attempt to incorporate a wider range of significant factors impacting migration robustness. These include void growth over time, the impact of initial residual stress, more accurate modelling of temperature influence on EM and SM, and temperature gradients resulting in TM. Those effects could be neglected in the past. Yet, their growing significance in advanced technology nodes demands for more sophisticated verification techniques and models.

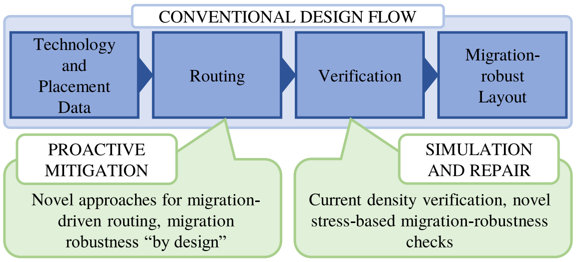
CONVENTIONAL DESIGN FLOW
Technology and Placement Data
Routing
Verification
Migration-robust Layout
PROACTIVE MITIGATION
Novel approaches for migration-driven routing, migration robustness "by design"
SIMULATION AND REPAIR
Current density verification, novel stress-based migration-robustness checks

Fig. 7. Migration robustness is checked during verification within conventional design flows. Traditional current density verification is more and more replaced by physics-based models [12]. Novel approaches consider migration-robustness constraints already in the routing step [4], [27], [28], [30].

B. CAD Flow for Migration-Robust Routing

Due to the increasing number of nets that are at danger of suffering EM-induced degradation, recent research does not only focus on precise and efficient modelling of migration mechanisms but also on novel design strategies. Those approaches attempt to avoid migration-induced wire degradation already during layout synthesis (Fig. 7). For instance, power grid synthesis can be performed by neural networks that have been trained considering EM constraints [27], [28]. Regarding signal lines, fast EM checks (e.g., [29]) can be included into the detailed routing step to estimate the hydrostatic stress and immediately implement appropriate countermeasures, if necessary. Another approach is to compose the interconnects of pre-verified routing segments [30]. As the verification is not part of the actual design process, extensive and precise simulation can be performed on each pattern. The routing algorithm is then constrained to those patterns and thereby generates a layout that is migration-robust "by design" [30].

C. Assessing Transistor Aging

The key challenge in estimating the impact of transistor aging on the delay of paths of a circuit is the large gap that exists between where aging does originate (i.e., different types of defects are being generated inside the transistor) and where aging effects ultimately manifest themselves at the circuit and system levels (i.e., errors due to induced timing violations). In order to bridge such a gap and accurately estimate the impact of aging, one has to start at the physical level, where defects originate. To do so, we employ state-of-the-art physics-based models to estimate the number of interface traps and oxide traps (i.e., generated defects) within nMOS and pMOS transistors caused by aging phenomena (BTI and HCI). More details are given in our prior works [31], [32].

Physics-based models, aside from their high accuracy (unlike empirical models), can estimate how various transistor's parameters can be degraded in the scope of any potential interdependencies [14], [15]. After estimating the number of generated defects, the corresponding degradations in the transistors' parameters can be estimated as follows [14]:

$$\Delta V_{th} = \frac{q}{C_{ox}} \cdot (\Delta N_{IT} + \Delta N_{OT}) \tag{3}$$

$$\Delta \mu = \frac{\mu_0}{1 + \alpha \cdot \Delta N_{IT}} \tag{4}$$

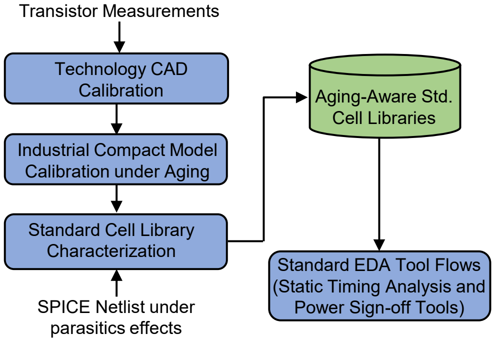
Transistor Measurements
Technology CAD Calibration
Industrial Compact Model Calibration under Aging
Standard Cell Library Characterization
SPICE Netlist under parasitics effects
Aging-Aware Std. Cell Libraries
Standard EDA Tool Flows (Static Timing Analysis and Power Sign-off Tools)

Fig. 8. Overview on creation of aging-aware standard-cell libraries, starting from semiconductor calibrating TCAD tool flow with transistor measurements to calibrating the compact model of MOSFETs, all the way to characterizing the standard-cell libraries. Libraries are fully compatible with the existing CAD tool flows (i.e., timing and power sign-offs).

Here, N_{IT} and ΔN_{OT} are the number of generated interface and oxide traps, respectively, obtained from [31]. q is the elementary charge, C_{ox} is the oxide capacitance of the transistor [14].

D. CAD Flow for Aging-Aware IC Design

1) Aging-Aware Standard-Cell Library: After estimating degradations induced by aging, we include the degraded parameters with the transistor compact model for the targeted technology node and perform standard-cell library characterization using commercial CAD tools (e.g., Synopsys SiliconSmart). The latter provides an *aging-aware cell library* [18], which includes the delay and power information for every standard cell. This library is fully compatible with the existing CAD flows for logic synthesis, timing optimization, power sign-off, etc. Thus, such an aging-aware library can be used directly within the design flow to both understand and handle aging-induced deviations for timing and power profiles.

In order to accurately capture the impact of aging on standard cells, we characterize every cell under different operating conditions (i.e., 7×7 input signal slews and output load capacitances), as typically done in commercial standard-cell libraries. In Fig. 8, we present an overview of how aging-aware libraries are created with the help of Technology CAD tool flows (e.g., Synopsys Sentaurus) to calibrate the industrial compact models of transistors (see further details in [32]).

2) Capturing the Impact of Time on Aging: The physics-based aging models can accurately estimate the interdependency of defect generation processes and time. Therefore, we can capture how degradations in the transistor parameter (i.e., V_{th}, μ) gradually evolve from the beginning of the circuit lifetime all the way until the projected end of the lifetime (e.g., 10 years). Then, the above-mentioned process of aging-aware cell library characterization can be analogously repeated for different time stamps from the beginning of the lifetime until to the end of the lifetime [2], [18].

3) Capturing the Impact of Activities on Aging: As mentioned earlier, aging-induced degradation depends on the duty cycle and hence the percentage of operation time in which the transistor was being under stress. Duty cycle is directly governed by the activities induced via the workloads that are being executed on the circuit. Therefore, different transistors across the circuit's netlist exhibit different duty cycles. To comprehend that fact, we can estimate the signal probabilities for the whole netlist using a gate-level simulator tool (e.g., Synopsys VCS). Then, using the SPICE netlist and the corresponding input/output signal probabilities, we can duty cycle every transistor within each standard cell. Finally, we perform characterization of every cell under the corresponding induced degradations [3], [6], [18].

4) Emerging Approaches: Standard-cell library characterization is a very time-consuming process because it necessitates large numbers of SPICE simulations. To accelerate the process of characterization, especially when it comes to modeling various workload profiles, machine learning (ML)-based approaches can be employed. With dedicated ML models, on-the-fly library characterization can be performed, replacing traditional SPICE simulations. In [2], [3], [33], we have demonstrated how ML-based library characterization provides several order of magnitude speedup with a very marginal loss of accuracy ($< 0.1\%$) for both delay and power information.

IV. Role of Reliability Effects for Security

A. Background: Security Threats

We provide a brief background on security threats relevant for the remainder of this paper. Please refer to [34], [35] for more details.

Trojans are malicious hardware modifications that are (i) targeting at the system level, register-transfer level (RTL), gate/transistor level, and/or the physical level; (ii) seeking to leak information from an IC, reduce the IC's performance, or disrupt an IC's working altogether; (iii) are always on, triggered internally, or triggered externally [36]. Most Trojans comprise a trigger and a payload; the trigger activates the payload on attack conditions, and the payload serves to perform the actual attack. Trojans are possibly introduced via third-party IP, by adversarial designers, or during mask generation or manufacturing, or even during distribution of ICs.

Side-channel attacks infer sensitive data, like encryption keys, from physical channels which are inevitably leaky due the nature of ICs in operation [37]. For example, the well-established AES cipher is vulnerable to power side-channel attacks (PSCAs), meaning that the AES key can be derived using statistical analysis on external power measurements [38].

Among others, there are circuit-level countermeasures proposed against both these threats, e.g., see [39]–[42]. However, few, if any, works consider security closure of physical layouts. That is, the assessment and hardening of the (literal) attack surfaces is overlooked so far.

B. Migration Effects: Threats and Attack Strategies

Migration effects seem most relevant for Trojans, fault-injection attacks, and side-channel attacks. For example, a wire under the influence of migration effects can exhibit increasing RC parasitics over time, which may aid side-channel attacks.

Here, we focus on the notion of migration effects-based Trojans—these are stealthy, zero-gate Trojans which have been largely overlooked in prior art. The characteristics of such Trojans can be described as follows.

- Migration effects-based Trojans, subsequently labeled as "ME Trojans," are targeting at the physical level, specifically at the interconnects. With the ME Trojan payload realized within the interconnects, such Trojans incur zero gate cost.[4] More specifically, payloads can be implemented as follows:
  – To leak information from an IC, e.g., via stuck-at faults in particular nets. This is achieved via failing wires, aiding subsequent sampling attacks, e.g., as in [43].
  – To reduce the IC's performance, by impacting the wire delay or IR drop of signal or clock nets, or by impacting the reliability of P/G nets.
  – To disrupt the IC's working, by rendering particular critical signal nets or P/G nets to fail.
- In advanced nodes, there are less margins for robust design. Thus, the threat of ME Trojans becomes even more concerning, as ME Trojans would require less efforts and could remain more likely undetected in advanced nodes.
- Unlike other types of Trojans, ME Trojans do not require functional activation. Thus, Trojan detection schemes based on regular testing is highly likely to be evaded, whereas burn-in testing may still detect or at least complicate the successful deployment of such Trojans.
- Given that state-of-the-art commercial verification approaches do not capture all mechanisms of migration effects (Sec. III-A), ME Trojans may be incorporated even early on, by adversarial designers.
- Given that migration effects are neither fully predictable nor entirely controllable, ME Trojans can exhibit considerable variation as to when they become effective. On the one hand, this limits the Trojans' scope for, e.g., controlled data leakage in the field. On the other hand, this renders the Trojans' particularly stealthy (especially for zero-gate implementations), as it can be difficult to differentiate their acting versus regular failures.

To implement ME Trojans, there are various options [7], [44], [45]. In principle, attackers want to take actions opposing to migration-robust design. For example, an attacker may

- increase local current densities, by modifying corners of wires, width of wires, dropping redundant vias, etc.;
- re-route nets as long wires, to undercut the Blech effect;
- modify reservoirs (i.e., passive wire segments)—i.e., add reservoir at the anode of wire segments or, if available, remove reservoirs from the cathode—to increase void growth by redistributing hydrostatic stress;
- modify an up-stream wire/via configuration to a downstream one, where early failures are more likely.

C. Migration Effects: Case Study on Trojans

Here, we review case studies of prior art [7], [45]. These studies focus on ME Trojans acting as malicious payload.

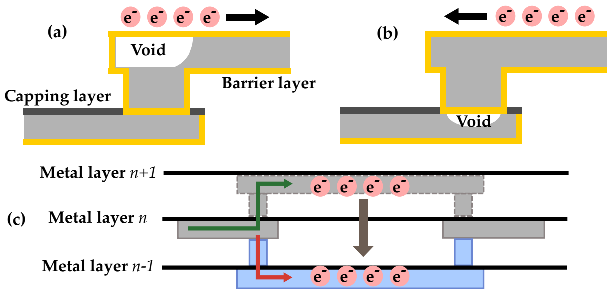

Fig. 9. (a) Via-below/upstream versus (b) via-above/downstream wire topologies. (c) The related Trojan attack, modifying a targeted-at upstream wire to a downstream wire, which is prone to early failures. Derived from [7].

1) Via-to-Wire Configurations: The placement of a via, with respect to the current flow's direction in the interconnect segment, significantly impacts the wire's time to failure (TTF). Wires with a via below, also known as upstream configuration, undergo a late failure process, after void nucleation [1], [7]. This is because the electron flow results in void formation in the upper metal layer's wire, where the current finds a path to flow for some time even after void nucleation. This is in contrast to the downstream configuration, i.e., via above the wire, with electron flow from higher to lower metal layer. There, the void is nucleated near the via interface and continued void growth can quickly and completely cut off conduction paths.

The void formation for both configurations is shown in Fig. 9, along with the Trojan implementation. In this attack, an upstream target wire is shifted down in the metal stack, making it a downstream wire that is prone to early failure [7]. A TTF reduction of $\sim$40% was reported for such an attack [7].

2) Cathode Reservoir: Consider a passive reservoir segment added to a wire's cathode. Such reservoirs are commonly employed to increase migration robustness, whereas they do not impact the IC's performance, power, or IR drop noticeably.

Now, a subtractive Trojan can stealthily degrade TTF by simply removing or by disabling the reservoir (the latter by passing an opposing current through). The impact of such Trojan attack on a $100\mu m \times 0.05\mu m$ wire was showcased in [45] where, after disabling a $50\mu m \times 0.1\mu m$ cathode reservoir, the nucleation time was reduced by up to 87%.

3) Anode Sink: In general, a sink at the anode would exacerbate the steady-state tensile stress at the cathode, thereby reducing the wire's TTF. Thus, an additive-Trojan attack works by inserting sinks to the target wire's anode.[5]

As with the cathode-reservoir removal attack, when adding a passive sink, the IC's performance, power, and IR drop remain largely unaffected. Such attacks are potent, considering that an initially immortal wire of size $20\mu m \times 0.05\mu m$ was shown to fail in $\sim$265 days with a passive anode sink of size $15\mu m \times 3\mu m$ inserted [7]. Further, using active, current-carrying sinks seems even more powerful, as the size of such sinks can be relatively small. For example, in [45] it was shown that, for

[4] Furthermore, migration effects can also be exploited as stealthy trigger, for other Trojans' gate-level payloads.

[5] Removing a cathode reservoir or inserting an anode sink ultimately impose the same threat vector, i.e., increasing the stress at the cathode.

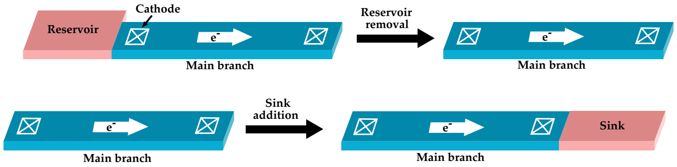

Fig. 10. Reservoir removal and sink addition Trojans. Metal segments, reservoir, and sink are not to scale. Derived from [7].

the same-sized immortal wire as above, adding an active anode sink of size $15\mu m \times 0.05\mu m$ reduces TTF to ~767 days.

Since the current density used for simulation is not given in [7], the TTF in both cases cannot be compared directly. On the one hand, the much smaller sink dimensions used to reach the wire's mortality in [45] emphasizes the effectiveness of active sinks for such attacks. On the other hand, an active sink is likely to impose noticeable impact on the IC's performance, power, and/or IR drop, hence, it can be easier to detect.

Figure 10 illustrates the two discussed Trojan attacks, i.e., the subtractive cathode-reservoir removal attack and the additive anode-sink insertion attack.

D. Transistor Aging: Threats and Attack Strategies

As explained earlier, transistor aging increases the transistor threshold voltage and decreases the carrier mobility; both effects impact the power and delay profiles of ICs. In practice, aged ICs exhibit less static and dynamic power as well as slower propagation delays. For one, the impact of aging on power has direct influence on the susceptibility to PSCAs. For another, the impact of aging on delay has influence on the susceptibility to timing errors which, in turn, can be exploited for attacks or leveraged for Trojan detection.

1) Power-Centric Attacks: It was found that aging can either undermine [46]–[48] or ease [49] different flavours of PSCAs, also depending on the circuitry under attack. These differing outcomes call for careful, security-centric consideration of aging and their impact on power profiles. In Sec. IV-E, we present such case study.

2) Timing-Centric Attacks: The works [50], [51] leverage dedicated, malicious workloads to accelerate aging-induced degradation much faster than what IC designers have estimated. For such unexpected scenarios, the guardbands can become insufficient, resulting in timing violations and hence errors during operation, which can be exploited subsequently.

E. Transistor Aging: Case Study on PSCA

As indicated, power side-channel attacks (PSCAs) are "powerful" threats given their non-invasiveness and proven effectiveness — and aging directly impacts the vulnerability of ICs against PSCAs. In this case study, we investigate and quantify the impact of aging for a 14nm FinFET library when under the seminal correlation power analysis (CPA) attack [38].

1) Setup: The aging-aware 14nm FinFET libraries have been characterized as described in Sec. III-D. The baseline library is derived from industrial measurement data. For aging effects, we consider a 50mV degradation in threshold voltage.[6]

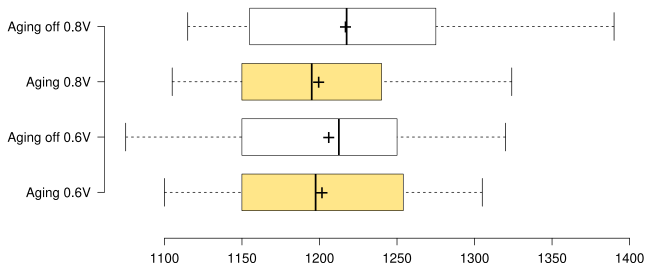

Fig. 11. Minimum number of traces to disclosure (MTTD) for 99.9% confidence of CPA attacks on a regular AES cipher module. Boxplots comprise results across 1,000 runs, with 10,000 randomized permutations of traces being considered for each run. Medians are represented by vertical bars, whereas means are represent by crosses.

We implement an integrated CAD and CPA framework for PSCA evaluation at design-time. As with library characterization, we leverage industry-standard CAD tools. We tackle the AES cipher, which is known to be prone to CPA attacks [38]. We use an AES RTL that works on 128-bit keys and 128-bit texts, uses look-up tables for the substitution box, and holds no dedicated PSCA countermeasure. The setup is described in more detail in [52]; the CAD and CPA framework, including the AES RTL, is publicly available in [53].

2) Results and Discussion: In Fig. 11, we illustrate the minimum number of traces to disclosure (MTTD) for different configurations, namely aging considered or ignored ("Aging off") with 0.6V or 0.8V supply voltage, all for the 14nm FinFET technology. We observe and argue the following:

- With aging considered, both 0.6V and 0.8V configurations approach a similar, more vulnerable level when compared to their respective counterparts ("Aging off").
- The drop in MTTD is more pronounced for the 0.8V configuration, implying that the aging effects, which are known to be stronger for higher voltages, can have indeed also a larger impact on PSCA resiliency.
- For both aging configurations, the MTTD variations are less, meaning that MTTD becomes more stable across the randomized sampling trials. This implies that aging works in favour of the CPA attack principle; this is because the dynamic power for different switching transitions becomes less differentiated after aging.

In short, aging effects have some detrimental impact on PSCA resilience. This calls for security-centric considerations of aging effects during the design of any sensitive IC.

V. Security Closure for Reliability Effects

As indicated, security closure means to conduct security-driven assessment and mitigation of layout-level threat vectors. Next, we discuss related strategies concerning reliability effects. We also outline a concept for CAD frameworks incorporating security closure. Recall that security closure in the broader context is further discussed in [8].

A. Strategies for Security Closure

To achieve security closure for reliability effects, one might initially want to follow best practices for mitigating these effects during design-time (Sec. III). However, doing so can be

[6] Such degradation can occur at different points in time, e.g., after 10 years at low voltage, temperature or after 3 years at high temperature, voltage, etc.

counterproductive sometimes and, in any case, is not enough—it is also essential to foresee and preempt malicious layouts modifications as best as possible.

1) Security Closure Strategies for Migration Effects: Recall the ME Trojan examples in Sec. IV-C. Here, security closure means to harden the routing such that security-critical wires

- are made robust enough otherwise, without cathode reservoirs, hindering the subtractive Trojan (Fig. 10 top);
- exhibit fully occupied tracks next to anodes, hindering the additive Trojan (Fig. 10 bottom); and
- exhibit fully occupied tracks in the layer(s) below, hindering the upstream-to-downstream Trojan (Fig. 9).

Similar measures may also apply for closure against other threats, like SCAs or FIAs, that exploit migration effects.

2) Security Closure Strategies for Aging: Recall the aging-centric attacks outlined in Sec. IV-D. Also recall the aging-aware library generation in Sec. III-D, which enabled us to study the impact of aging on the CPA attack in Sec. IV-E.

Given this context, security closure can be initiated already early on in the CAD flow, that is, during logic synthesis. In other words, providing the synthesis tool with aging-aware standard-cell libraries would enable synthesis to optimize the circuit's netlist as desired in the presence of aging-induced degradations.[7] Here, synthesis should be configured, e.g., to mitigate PSCAs by either fully balancing or randomizing the power consumption (both to mitigate the related information leakage) for different switching transitions.

Still, such early closure efforts must be maintained throughout the CAD flow (as motivated in general in [35]), also given the sensitivity of physical layouts to reliability effects. Follow-on closure measures for layouts should, e.g., to mitigate PSCAs maintain power balancing carefully via gate sizing, placement and routing, etc. Such closure measures are even still needed for dedicated circuit-level countermeasures [54].

B. CAD Frameworks for Security Closure

Note that the above strategies can conflict with traditional CAD optimization and/or exacerbate other threats. For example, while heavily occupying routing tracks seems desirable for utilization of the metal stack (and provides security closure against the discussed ME Trojans), doing so is challenging for routing tools, especially for large designs using advanced technology nodes with ever-more complicated routing rules. Besides, heavily utilized tracks may also ease cross-coupling and glitching attacks [55], although this threat still depends primarily on routing patterns for victim and aggressor wires.

Thus, security closure of physical layouts represents a significant challenge that must be addressed via well-coordinated efforts within CAD flows, focusing on physical design in particular. We outline a concept for CAD frameworks incorporating security closure in Fig. 12. At their heart, such frameworks should leverage regular, commercial CAD tools—doing so is preferable in any case, but also practical, given the scriptability of CAD tools. That is, means for sign-off-grade assessment as well as mitigation of layout-level security threats can be linked into the CAD flow via tool scripting. For a start of such scripting efforts, established means for mitigation of reliability effects can be leveraged, but need to be carefully re-tailored to support (and not contradict) security closure.

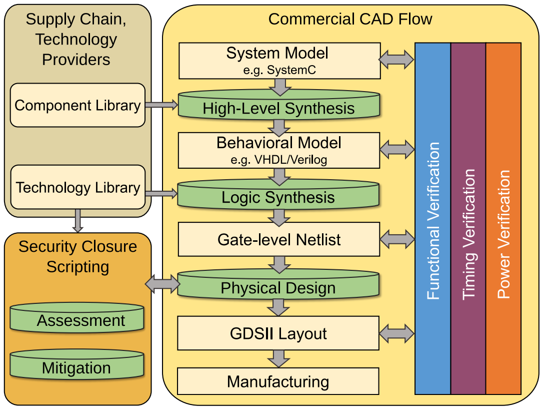

Fig. 12. Proposed CAD flow with means for security closure of physical layouts.

VI. Conclusion and Outlook

In this paper, we took a security-centric view on reliability effects, in particular on migration effects in interconnects and aging effects in transistors. Based on a thorough review of the effects' working principles, we studied particular security threats arising from those effects. These kinds of threats are stealthy and hard to manage, requiring dedicated efforts directly at the physical and layout level where they occur. Such efforts, however, have been overlooked in prior art. Accordingly, we introduce and call for *security closure of physical layouts* in the face of reliability effects. Our future work is to (i) implement and conduct experimental studies on sign-off-grade means for assessment and mitigation of such threats within CAD flows and (ii) engage the security and CAD communities for independent verification and validation.

Beyond the notion of security closure of physical layouts, we argue that CAD frameworks should consider security even more holistically, as in aiming for *secure-by-design* [35]. Such efforts must be starting from the specification and behavioral design, all the way down to the physical layouts—where security closure would take over—along with feedback loops for CAD stages as needed. Realizing such holistic frameworks for secure-by-design flows would require (i) continuous top-down propagation and translation of security requirements and specifications, and (ii) bottom-up verification of security metrics against attackers' capabilities and limitations.

Acknowledgement

This work was supported in part by the US Office of Naval Research, Grant N00014-18-1-2672, and in part by the German Research Foundation (DFG), project "ACCROSS: Approximate Computing aCROss the System Stack."

[7] Generally, the synthesis tool will prefer (avoid) gates that exhibit less (larger) delay increases in the presence of aging effects. Note that, even under the same degree of aging, different gates will exhibit different delay increase; hence the need for full library generation. In [18], [32], we study the effectiveness of aging-aware (but security-unaware) logic synthesis, demonstrating circuits that exhibit around 50% more efficiency compared to convectional approaches using timing guardbands.

References

[1] J. Lienig and M. Thiele, *Fundamentals of Electromigration-Aware Integrated Circuit Design*. Springer, 2018. [Online]. Available: https://www.springer.com/us/book/9783319735573

[2] F. Klemme and H. Amrouch, "Machine learning for on-the-fly reliability-aware cell library characterization," *Trans. Circ. Sys. I*, vol. 68, no. 6, pp. 2569–2579, 2021.

[3] ——, "Machine learning for circuit aging estimation under workload dependency," in *Proc. Int. Test Conf.*, 2021.

[4] S. Bigalke and J. Lienig, "Avoidance vs. repair: New approaches to increasing electromigration robustness in VLSI routing," *Integration*, vol. 75, pp. 189 – 198, 2020. [Online]. Available: https://doi.org/10.1016/j.vlsi.2020.04.009

[5] J. Lienig and M. Thiele, "The pressing need for electromigration-aware integrated circuit design," in *Proc. ISPD*, 2018, pp. 144–151. [Online]. Available: https://doi.org/10.1145/3177540.3177560

[6] A. Thirunavukkarasu *et al.*, "Device to circuit framework for activity-dependent NBTI aging in digital circuits," *Trans. Electron Dev.*, vol. 66, no. 1, pp. 316–323, 2018.

[7] C. Cook, S. Sadiqbatcha, Z. Sun, and S. X.-D. Tan, "Reliability based hardware Trojan design using physics-based electromigration models," *Integration*, vol. 66, pp. 9–15, 2019.

[8] J. Knechtel *et al.*, "Security closure of physical layouts," in *Proc. ICCAD*, 2021.

[9] S. Chatterjee, V. Sukharev, and F. N. Najm, "Power grid electromigration checking using physics-based models," *Trans. Comp.-Aided Des. Integ. Circ. Sys.*, vol. 37, no. 7, pp. 1317–1330, 2018.

[10] I. A. Blech, "Electromigration in thin aluminum films on titanium nitride," *J. Appl. Phys.*, vol. 47, no. 4, pp. 1203–1208, 1976.

[11] J. Black, "Electromigration—a brief survey and some recent results," *Trans. Electron Dev.*, vol. 16, no. 4, pp. 338–347, 1969.

[12] M. A. Korhonen, P. Børgesen, K. N. Tu, and C. Li, "Stress evolution due to electromigration in confined metal lines," *J. Appl. Phys.*, vol. 73, no. 8, pp. 3790–3799, 1993.

[13] M. I. Khan, A. R. Buzdar, and F. Lin, "Self-heating and reliability issues in FinFET and 3D ICs," in *Proc. Int. Conf. Sol.-St. Int. Circ. Tech.*, 2014.

[14] H. Amrouch *et al.*, "Towards interdependencies of aging mechanisms," in *Proc. ICCAD*, 2014, pp. 478–485.

[15] H. Amrouch *et al.*, "Impact of BTI on dynamic and static power: From the physical to circuit level," in *Proc. Int. Rel. Phys. Symp.*, 2017, pp. CR–3.

[16] V. Surabhi *et al.*, "Exposing hardware Trojans in embedded platforms via short-term aging," *Trans. Comp.-Aided Des. Integ. Circ. Sys.*, 2020.

[17] H. Amrouch, "Techniques for aging, soft errors and temperature to increase the reliability of embedded on-chip systems," Ph.D. dissertation, 2015.

[18] H. Amrouch, B. Khaleghi, A. Gerstlauer, and J. Henkel, "Reliability-aware design to suppress aging," in *Proc. DAC*, 2016, pp. 1–6.

[19] S. Bigalke *et al.*, "The need and opportunities of electromigration-aware integrated circuit design," in *Proc. ICCAD*, 2018, pp. 1–8.

[20] F. N. Najm and V. Sukharev, "Efficient simulation of electromigration damage in large chip power grids using accurate physical models (invited paper)," in *Proc. Int. Rel. Phys. Symp.*, 2019, pp. 1–10.

[21] "Cadence Spectre APS," https://community.cadence.com/cadence_blogs_8/b/cic/posts/using-spectre-aps-for-analysing-emir.

[22] "ANSYS RedHawk-SEM," https://www.apache-da.com/products/redhawk/redhawk-sem.

[23] M. Thiele, S. Bigalke, and J. Lienig, "Exploring the use of the finite element method for electromigration analysis in future physical design," in *Proc. VLSI-SoC*, 2017, pp. 1–6.

[24] A. Abbasinasab and M. Marek-Sadowska, "RAIN: A tool for reliability assessment of interconnect networks–physics to software," in *Proc. DAC*, 2018, pp. 1–6.

[25] Z. Sun *et al.*, "EMSpice: Physics-based electromigration check using coupled electronic and stress simulation," *Trans. Dev. Mat. Rel.*, vol. 20, no. 2, pp. 376–389, 2020.

[26] S. Torosyan *et al.*, "Novel physics-based tool-prototype for electromigration assessment in commercial-grade power delivery networks," *J. Vacuum Sci. & Tech. B*, vol. 39, no. 1, p. 013203, 2021.

[27] S. Dey, S. Nandi, and G. Trivedi, "PowerPlanningDL: Reliability-aware framework for on-chip power grid design using deep learning," in *Proc. DATE*, 2020, pp. 1520–1525.

[28] V. A. Chhabria *et al.*, "Template-based PDN synthesis in floorplan and placement using classifier and CNN techniques," in *Proc. ASPDAC*, 2020, pp. 44–49.

[29] Z. Sun *et al.*, "Voltage-based electromigration immortality check for general multi-branch interconnects," in *Proc. ICCAD*, 2016, pp. 1–7.

[30] M. Thiele, S. Bigalke, and J. Lienig, "Electromigration analysis of VLSI circuits using the finite element method," in *VLSI-SoC: Opportunities and Challenges Beyond the Internet of Things*. Springer, 2019, pp. 133–152.

[31] S. Mahapatra and N. Parihar, "Modeling of NBTI using BAT framework: DC-AC stress-recovery kinetics, material, and process dependence," *Trans. Dev. Mat. Rel.*, vol. 20, no. 1, pp. 4–23, 2020.

[32] S. Mishra *et al.*, "A simulation study of NBTI impact on 14-nm node FinFET technology for logic applications: Device degradation to circuit-level interaction," *Trans. Electron Dev.*, vol. 66, no. 1, pp. 271–278, 2018.

[33] F. Klemme, Y. Chauhan, J. Henkel, and H. Amrouch, "Cell library characterization using machine learning for design technology co-optimization," in *Proc. ICCAD*, 2020, pp. 1–9.

[34] J. Knechtel, "Hardware security for and beyond CMOS technology," in *Proc. ISPD*, 2021, pp. 115–126.

[35] J. Knechtel *et al.*, "Towards secure composition of integrated circuits and electronic systems: On the role of EDA," in *Proc. DATE*, 2020, pp. 508–513.

[36] S. Bhunia and M. M. Tehranipoor, Eds., *The Hardware Trojan War: Attacks, Myths, and Defenses*. Springer, 2018.

[37] Y. Zhou and D. Feng, "Side-channel attacks: Ten years after its publication and the impacts on cryptographic module security testing," in *IACR Crypt. ePrint Arch.*, no. 388, 2005.

[38] E. Brier, C. Clavier, and F. Olivier, "Correlation power analysis with a leakage model," in *Trans. Cryptogr. Hardw. Embed. Sys.*, 2004.

[39] D. Bellizia *et al.*, "Secure double rate registers as an RTL countermeasure against power analysis attacks," *Trans. VLSI Syst.*, vol. 26, no. 7, pp. 1368–1376, 2018.

[40] F. Zhang *et al.*, "Design and evaluation of fluctuating power logic to mitigate power analysis at the cell level," *Trans. Comp.-Aided Des. Integ. Circ. Sys.*, 2020.

[41] K. Xiao, D. Forte, and M. Tehranipoor, "A novel built-in self-authentication technique to prevent inserting hardware Trojans," *Trans. Comp.-Aided Des. Integ. Circ. Sys.*, vol. 33, no. 12, pp. 1778–1791, 2014.

[42] L. A. Guimarães, R. P. Bastos, and L. Fesquet, "Detection of layout-level Trojans by monitoring substrate with preexisting built-in sensors," in *Proc. Comp. Soc. Symp. VLSI*, 2017, pp. 290–295.

[43] J. Pan, F. Zhang, K. Ren, and S. Bhasin, "One fault is all it needs: Breaking higher-order masking with persistent fault analysis," in *Proc. DATE*, 2019, pp. 1–6.

[44] A. Sreedhar, S. Kundu, and I. Koren, "On reliability Trojan injection and detection," *J. Low Power El.*, vol. 8, no. 5, pp. 674–683, 2012.

[45] S. Tan, Z. Sun, and S. Sadiqbatcha, "Interconnect electromigration modeling and analysis for nanometer ICs: From physics to full-chip," *Trans. Sys. LSI Des. Method.*, vol. 13, pp. 42–55, 2020.

[46] N. Karimi, T. Moos, and A. Moradi, "Exploring the effect of device aging on static power analysis attacks," *Trans. Cryptogr. Hardw. Embed. Sys.*, vol. 2019, no. 3, pp. 233–256, 2019.

[47] T. Kroeger *et al.*, "Effect of aging on PUF modeling attacks based on power side-channel observations," in *Proc. DATE*, 2020, pp. 454–459.

[48] F. Niknia, J.-L. Danger, S. Guilley, and N. Karimi, "Aging effects on template attacks launched on dual-rail protected chips," *Trans. Comp.-Aided Des. Integ. Circ. Sys.*, pp. 1–1, 2021.

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

[50] N. Karimi *et al.*, "Magic: Malicious aging in circuits/cores," *Trans. Arch. Code Opt.*, vol. 12, no. 1, pp. 1–25, 2015.

[51] H. Amrouch *et al.*, "Emerging (un-)reliability based security threats and mitigations for embedded systems," in *Proc. Compiler Arch. Synth. Emb. Sys.*, 2017, pp. 1–10.

[52] J. Knechtel *et al.*, "Power side-channel attacks in negative capacitance transistor," *Micro*, vol. 40, pp. 74–84, 2020.

[53] J. Knechtel. (2019–2020) Correlation power attack. [Online]. Available: https://github.com/DfX-NYUAD/CPA

[54] D. Fujimoto *et al.*, "Correlation power analysis using bit-level biased activity plaintexts against AES cores with countermeasures," in *Proc. Int. Symp. Electromag. Comp.*, 2014, pp. 306–309.

[55] C. Kison, O. M. Awad, M. Fyrbiak, and C. Paar, "Security implications of intentional capacitive crosstalk," *Trans. Inf. Forens. Sec.*, 2019.