A Novel Attack Mode on Advanced Technology Nodes Exploiting Transistor Self-Heating

Nikhil Rangarajan *Member, IEEE*, Johann Knechtel, *Member, IEEE*, Nimisha Limaye, *Student Member, IEEE*, Ozgur Sinanoglu, *Senior Member, IEEE*, and Hussam Amrouch, *Member, IEEE*

***Abstract*—Self-heating (SH) is a phenomenon that can induce excessive heat inside the transistor channel. SH represents an emerging and serious concern especially in advanced technology nodes, where excessive heat acting on elevated channel geometries will notably shift the critical transistor parameters (e.g., threshold-voltage V_{th} and carrier mobility μ). The underlying 3-D device structures (e.g., FinFET, nanowire, or nanosheet structures), along with newly-employed materials like silicon-germanium (SiGe), which show worse thermal conductivity than traditional materials, can considerably exacerbate SH. On top of that, quantum confinement, a phenomenon that becomes dominant at sub-10nm, further increases the intensity of SH.**

In this paper, we are the first to explore SH effects from the perspective of hardware security, rather than the performance, reliability standpoints covered in state-of-the-art (SOTA) work. As proof of concept, we devise a SH-based hardware Trojan (HT) that exploits the SH-induced V_{th} change in 7nm FinFET circuits. Leveraging V_{th}-dependent reconfigurable logic, we design a reconfigurable HT payload that maliciously changes its functional behavior once the SH-induced V_{th} change takes effect.

Following SOTA work, we present a comprehensive modeling and analysis of SH effects at the device-level, and highlight its impact on transistor V_{th}. Next, we study how fabrication-time changes in the transistor doping and geometry can promote the SH-assisted degradation. We then describe various payload configurations for the proposed HT, quantify its overheads, and discuss its resilience against standard HT detection techniques. Finally, we demonstrate two case studies using the proposed HT, one to leak the secret key from a pipelined design of an advanced encryption standard (AES) circuit, and another to showcase denial-of-service for a Gaussian-blur filter circuit. Our work utilizes industry-standard models with parameters extracted from measurements and calibrated with experiments. Our results are obtained from meticulous study and optimization across the device-, circuit-, and system-levels.

***Index Terms*—Self-Heating, Transistor Aging, Hardware Trojan, AES, Reconfigurable Logic.**

I. Introduction

The design challenges of technology scaling beyond the sub-10nm regime are becoming more and more pronounced. For example, power density constraints limit the ever-closer integration of transistors and rather necessitate the adoption of new strategies like gate-all-around (GAA) structures [1], nanosheet devices [2], or 3D stacking [3], among others. Even the ubiquitous FinFET technology, which is used in most modern electronics, is plagued by thermal limitations owing to increased power density and thermal resistance. The resulting self-heating (SH) effects can induce excessive heat inside the transistor channel [4], [5]. SH effects have become a critical concern for performance and reliability for advanced nodes [6], [7], via a combination of phenomena like negative-bias temperature instability (NBTI), electromigration (EM), and hot-carrier injection (HCI) [8].

The main contributing factor for SH effects in confined transistor geometries like FinFET and GAA configurations is the increasing thermal resistance of the channel, which is aggravated by the use of high-κ gate dielectrics and high-mobility channels [8]. The shrinking of channel dimensions results in an even more significant reduction of the channel's thermal capacitance, thus reducing the overall thermal time constant or, in other words, the time it takes for the channel to heat up. This issue, coupled with the reliability effects (NBTI, EM, HCI, etc.) borne out of it, all compound for the degradation of the transistors' electrical characteristics, including the threshold-voltage (V_{th}), subthreshold slope, and carrier mobility [9]. Various other factors further impact SH-induced transistor degradation, including doping and fin topology.

Apart from the above performance and reliability concerns, SH can also become a critical challenge from the standpoint of hardware security. Note that security vulnerabilities arising at the device-level are easily exacerbated at the system-level unless the device-level root causes are mitigated. Such repercussions may include denial of service (DoS) during operation, increased leaking of sensitive data at runtime, or leaking of intellectual property of circuit design.

In this paper, we are the first to explore the outlined novel attack mode on advanced technology nodes exploiting SH effects. More specifically, we study the scenario of a hardware Trojan (HT) designed to exploit SH effects in sub-10nm transistor topologies with the intent to compromise the system-level security and functionality of exemplary designs.

Threat model: Consider the classical HT threat model in Fig. 1(a). Here, all entities in the supply chain, including the

Manuscript received April 07, 2022; revised June 11, 2022; accepted July 05, 2022. This article was presented in the International Conference on Compilers, Architectures, and Synthesis for Embedded Systems (CASES) 2022 and appears as part of the ESWEEK-TCAD special issue.

Nikhil Rangarajan, Johann Knechtel, and Ozgur Sinanoglu are with the Division of Engineering, New York University Abu Dhabi, Saadiyat Island, 129188, UAE. (email: nikhil.rangarajan@nyu.edu, johann@nyu.edu, ozgursin@nyu.edu).

Nimisha Limaye is with the Department of Electrical and Computer Engineering, Tandon School of Engineering, New York University, Brooklyn, NY, 11201, USA. (email: nimisha.limaye@nyu.edu).

Hussam Amrouch is with the Chair for Semiconductor Test and Reliability (STAR) in the Computer Science, Electrical Engineering Faculty at the University of Stuttgart, Stuttgart 70569, Germany. (email: amrouch@iti.uni-stuttgart.de)

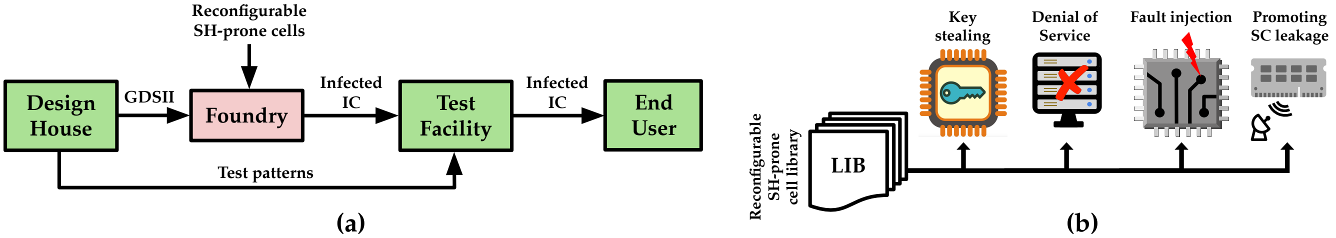


Fig. 1: (a) Threat model for the proposed HT exploiting the novel SH-based attack mode. The foundry (red) is considered untrusted while all other entities are trusted (green). This is the classical threat model for HTs. (b) Scope and threat scenarios arising from the proposed HT.

design house, test facility and end-user, are trusted; only the foundry is untrusted and assumed to embed some HTs. More specifically, for this work, the malicious entities residing in the foundry integrate SH-prone and reconfigurable HT cells into the design to be fabricated. These HT cells can either replace existing gates in the original design or be a stealthy addition.

The HT cells are specifically designed (by us, the authors, taking the stand of the malicious entities) such that they retain their original electrical characteristics and logical functionality for a period long enough to thwart detection at the test facility. After field deployment, the impact of SH effects accrue over time and cause the transistors' V_{th} to degrade, which changes its functionality. The transformation carries over to the circuit-level and thus enables the malicious entities to enact various attack vectors like key stealing, DoS, fault injection or promoting side-channel (SC) leakage (Fig. 1(b)).

Related Work: Reconfigurable and/or polymorphic behavior arising at the device-level have been explored in the context of hardware security in various prior art, both for defense and attack schemes; selected examples follow. Silicon nanowire (SiNW) FETs leveraging ambipolarity to achieve reconfigurability were employed for layout obfuscation in [10]. The intrinsic polymorphic behavior in spin-based devices has enabled both static and dynamic camouflaging schemes [11], [12]. A polymorphic HT based on hybrid spin-CMOS architectures was proposed in [13]. However, the application of such HT is limited since hybrid spin-CMOS systems are not well established currently. V_{th}-dependent reconfigurable gates for IC camouflaging have been investigated in [14]–[16]. Recently, [17], [18] studied circuit reliability and physical design in advanced nodes which both bring profound challenges to hardware security.

In the past few years, SH phenomenon has been largely researched in the device physics community. For example, [8] studied in detail how SH impacts advanced technology nodes and focused on how abstracted models can be developed. More importantly, authors showed the strong relation between SH and transistor aging mechanisms, demonstrating how excessive heat caused by SH can considerably accelerate the generation of defects. In [9], authors demonstrated how SH models can be calibrated and incorporated with the industry-standard compact model of FinFET technology. They also showed for the first time how SH is a concern not only for analog circuits but for digital circuits as well. Recently, [5], [19] studied the impact of SH on the 14nm FinFET technology node as well as 14nm nanowire after careful calibration with semiconductor measurement data. An example of how SH impacts FinFET and nanowire devices is presented in Fig. 2(b).

Our novel contributions: In this paper, we propose a novel HT design that utilizes SH-induced V_{th} modulation to implement reconfigurable payloads in conventional FinFET circuits. The main contributions of this work are as follows.

1) To the best of our knowledge, this is the first work to demonstrate a reconfigurable SH-based HT for conventional FinFET systems.
2) We study the SH effects in confined FinFET geometries using industry standard models, analyze the effect of fin number on SH, and the temporal evolution of the V_{th} shift in 7nm FinFETs.
3) We provide a methodology for foundry-based attackers to achieve a desired trigger time for the SH-based HT, by tuning the thermal resistance as a function of the payload transistors' doping and metal work function.
4) We examine the feasibility of various payload configurations implemented with different baseline V_{th} levels.
5) We highlight the system-level repercussions of the proposed HT design through case studies on secret-key retrieval in an advanced encryption standard (AES) design and a DoS attack for an image processing module.

II. Self-Heating in FinFET Technology

A. Background

1) Self-Heating Effects:
Due its effective gate control (which suppresses short-channel effects), excellent transport properties, and high $I_{\text{ON}}/I_{\text{OFF}}$ ratio, the FinFET structure has enabled the continuous scaling of transistors. Nevertheless, the nano-scaled dimensions along with confined 3-D structures make FinFET transistors suffer from an ever-increasing current density inside the channel. Hence, FinFET transistors are inevitably subject to degradations caused by electro-thermal (ET) effects like SH—especially at the 14nm node and below (see Fig. 2). The primary mechanism that induces SH is carrier-phonon interaction, especially near the drain-to-channel junction where an exaggerated electric field occurs.

SH effects arise due to the limited silicon volume for heat dissipation during operation (i.e., when the current flows inside the channel during switching) and the low thermal conductivity of high-κ materials used to build the gate oxide. The problem is further exacerbated when the transistor geometries are aggressively scaled down (e.g., 7nm) [21] and/or more confined

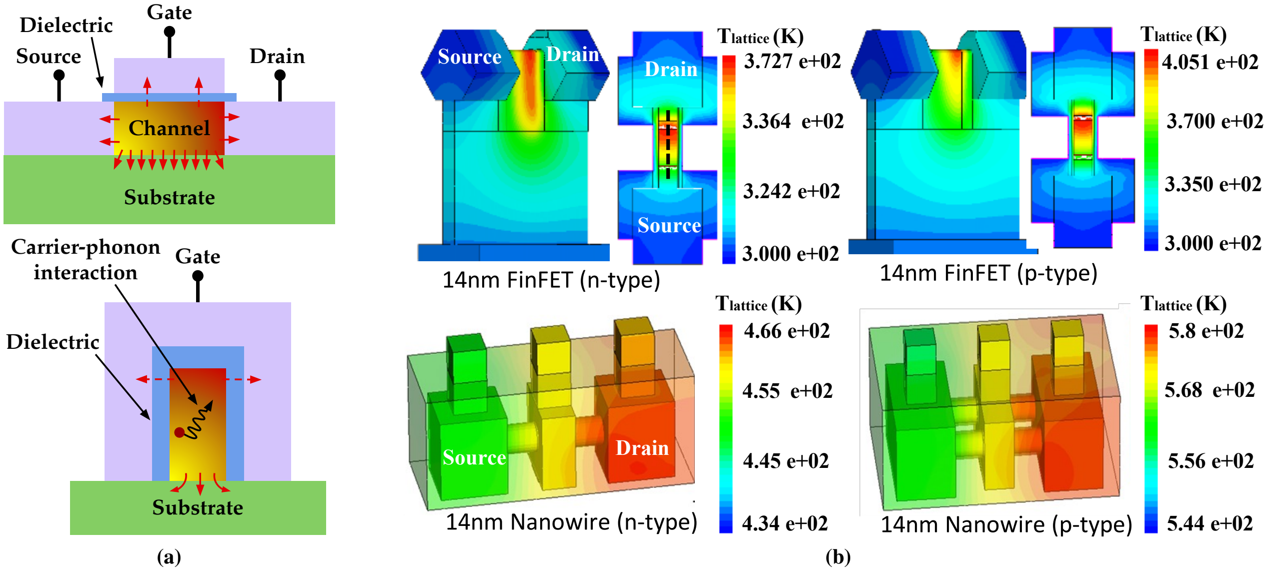


Fig. 2: (a) Effective multi-directional heat dissipation in planar MOSFETs (top) as compared to limited heat dissipation in FinFET geometry (bottom) [20]. Moreover, the carrier-phonon interaction in the confined FinFET channel generates more heat. (b) Thermal profiles showing the impact of self-heating in 14nm FinFET technology [5] as well as 14nm nanowires [19]. As shown, advanced technology nodes suffer from a significant increase in the temperature of the channel, due to the quantum confinement.

3-D structures are adopted, like nanowires [19] and even in emerging negative capacitance transistors NCFETs [22]. The heat transport across the channel of such devices is quasi-1-D (i.e., the current flows from drain to source in one dimension akin to the tiny diameter and length of the channel) [23].

SH impacts the electrical characteristics of both n-type and p-type FinFET transistors in both short- and long-terms. In the short-term (i.e., in the order of microseconds), the heat generated inside the transistor's channel leads to a reduction in carrier mobility. This is mainly because, at elevated temperatures, phonon scattering increases, which reduces the probability of a carrier to find a free path to move from the source to drain. In the long-term (i.e., in the order months or years), the accumulated effects of elevated temperatures accelerate the major underlying mechanisms of defects generation (e.g., interface trap generation due to the breakdown of Si-H bounds at the interface). Hence, transistors age faster due to BTI and HCI. In practice, the generated defects manifest themselves as undesired charges, which leads to a noticeable increase in the threshold-voltage (V_{th}) [8].

In this work, the long-term impact of SH forms the fundamental mechanism that we employ to *considerably accelerate* the aging-induced increase of threshold-voltages. *This, in practice, serves as trigger for the proposed HT.*

2) *Underlying Aging Mechanisms:*

Bias temperature Instability (BTI) and hot-carrier injection (HCI) are considered the major aging mechanisms that seriously degrade the reliability of MOSFET transistors in current and upcoming technology nodes. In the following, we briefly explain how the BTI and HCI phenomena occur and why elevated temperatures caused by SH considerably stimulate and accelerate them.

BTI occurs when the vertical electric field is applied to form the channel of a transistor, namely when some of the abundant Si-H bonds at the interfacial layer (i.e., Si-SiO$_2$) are broken down due to the induced stress. The hydrogen ion (H^+) then defuses and moves away, leaving the silicon ion (Si$^+$) as undesired charge at the interfacial layer. In addition, some of the carriers that are being attracted during the channel formation may obtain enough energy and to be tunneled to the oxide layer (i.e., the high-κ layer) in which they are then captured by the available oxide vacancies (i.e., the pre-existing defects during fabrication). Both interface traps and oxide traps are undesired charges that will be accumulated over time and, hence, weaken the vertical electrical field when it is applied to tune the transistor on. Therefore, in practice, a higher voltage would be necessary to switch the transistor from the OFF to the ON state. As a result, BTI manifests itself as an *increase in the transistor threshold voltage* (V_{th}). Further, the undesired charges induced by the interface traps distributed across the channel interact with the charges that were attracted to form the transistor's channel, leading to a reduction in the carrier mobility due to Coulomb scattering. In sub-45nm technology nodes, BTI impacts both nMOS and pMOS transistors and results in a gradual increase in V_{th} from the beginning until the end of the lifetime.

HCI occurs when the lateral electric field is applied, in which accelerated carriers across the transistor's channel may get "hot" and then be injected near the transistor drain area.[1] Such injected carriers result in breaking of Si-H bonds and, hence, additional interface traps. Similar to BTI, HCI-induced interface traps get accumulated over time, leading to a further increase in V_{th}. Both BTI and HCI have a strong, namely exponential dependency to temperature. This is because elevated temperatures do accelerate the underlying chemical reactions that are responsible of breaking of the Si-H bonds. Further, elevated temperature provide additional activation energy that

[1] Note that "hot" in this context does not refer to the temperature but rather to the obtained kinetic energy from the acceleration mechanism itself.

TABLE I: SH Parameters extracted from the available data in [9], [26]. Calibrated R_{th0} and C_{th0} for the BSIM-CMG compact model.

Parameter	1 Fin	3 Fins	7 Fins
R_{th0}	5.44e-2	1.63e-1	2.95e-1
C_{th0}	1.83e-6	6.12e-7	3.37e-7
$fpitch$	2.7e-8	2.7e-8	2.7e-8
ASHEXP	0.249	0.249	0.249
BSHEXP	1	1	1

leads to more defect generation. Thus, transistor SH, which is the key focus of this work, plays a major role in accelerating both BTI and HCI mechanisms. Hence, under the impact of SH, a certain degradation (i.e., a certain amount of ΔV_{th} can be reached within much shorter time. BTI-induced degradation (i.e., ΔV_{th}) is also subject to the activities caused by the running workloads on top of the circuit [24]. Nevertheless, temperature increase has a much stronger and dominant impact than the duty cycles induced by the running workloads.

B. Self-Heating in 7nm FinFET Technology

1) Modelling and Parameters:

The increase in the channel temperature (ΔT_{C}) induced by SH effects depends on two main factors; the amount of generated heat and the heat dissipation. On the one hand, the generated heat is a direct result of the power loss across the channel: $P_{\text{loss}} = I_{\text{D}} \cdot V_{\text{DS}}$ [8]. On the other hand, the heat dissipation mechanism is determined by the thermal resistance (R_{th}) and thermal capacitance (C_{th}) of the FinFET device [9], [25]. In practice, the dielectric material, fin structure/size, metal contact resistance, etc. determine both R_{th} and C_{th} [8] [26]. Also note that the doping concentration of the transistor channel plays a major role in determining the amount of heat generated by SH because it directly impacts the thermal resistance of the channel and hence the power losses [8].

The industry-standard compact model of FinFET technology (BSIM-CMG) [25] models SH through an RC-thermal network. The BSIM-CMG parameters R_{th0} and C_{th0} must be calibrated to reflect the $R_{\text{th}}, C_{\text{th}}$ extracted from measurements. To this end, we employ the measurements for the 7nm FinFET technology provided by IMEC [26]. In order to capture the impact of fin numbers on SH, we have modeled R_{th} as a function of #fins based on the measurement data in [26]. We have incorporated the dependency of SH on the number of fins through parameters (ASHEXP and BSHEXP) available within the BISM-CMG FinFET model [9], [25], as follows:

$$R_{\text{th}}(\#\text{fins}) = \frac{R_{\text{th0}}}{W_{\text{th0}} \cdot \#\text{fingers}^{\text{BSHEXP}} + fpitch \cdot \#\text{fins}^{\text{ASHEXP}}} \tag{1}$$

Then, the thermal capacitance (C_{th}) is modeled as

$$C_{\text{th}} = \frac{\tau_{\text{th}}}{R_{\text{th}}(\#\text{fins})}, \tag{2}$$

where τ_{th} is considered to be 100 ns [26], [27].

In Table I, we summarize the calibrated $R_{\text{th}}, C_{\text{th}}$ values, which are later employed within the BSIM-CMG to model and capture SH effects. This enables us to estimate the amount of heat generated through SH in the transistor's channel.

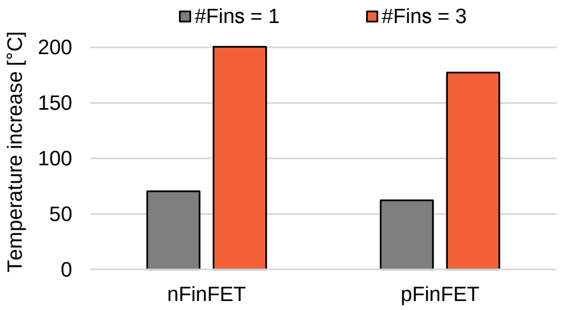


Fig. 3: Temperature increase within the channel of nFinFET and pFinFET transistors due to self-heating effects. Results obtained from accurate SPICE simulations using the industry-standard compact model after a careful calibration of SH parameters against measurements. A higher number of fins leads to a larger current densities and hence more excessive SHE.

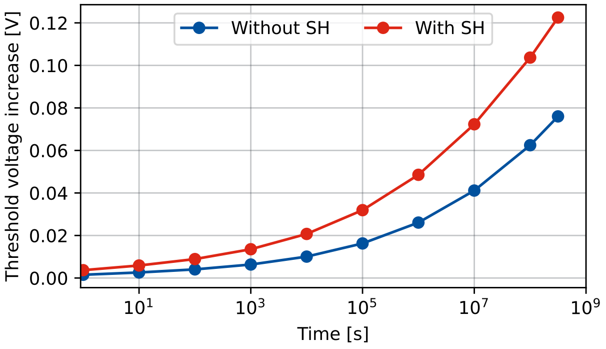


Fig. 4: Aging-induced threshold-voltage increase over time. Self-heating accelerates aging and therefore a larger degradation (i.e., V_{th} increase) can be induced. Therefore, SHE can be exploited to accelerate aging and reach a certain level of degradation but at a much earlier time. A detailed analysis on how to achieve that is presented later in Fig. 6.

2) Analysis:

To estimate the impact of SH on the temperature of FinFET devices, both n-type and p-type, we employ accurate SPICE simulations using the BSIM-CMG model after calibrating SH model parameters. This enables us to extract the temperature of the transistor's channel, which the FinFET device exhibits during the operation.

In Fig. 3, we demonstrate how SH can cause a considerable increase in the transistor temperature. In the case of a FinFET with merely 1 fin, the temperature increases by around 70°C and 60°C for the case of nFinFET and pFinFET, respectively. More importantly, when a higher number of fins is employed, the temperature increase becomes more severe, reaching 201°C and 177°C, for the case of nFinFET and pFinFET, respectively.

Recall that the underlying key mechanisms contributing to transistor aging are BTI and HCI. Both of them lead to an increase in V_{th} due to the generated defects. Importantly, transistor aging has an exponential dependency on the operating temperature. In Fig. 4, we can see how aging-induced threshold-voltage increase (ΔV_{th}) progresses with and without SH effects. As can be noticed, SH noticeably accelerates aging. For instance, a ΔV_{th} of 80 mV, which cannot be achieved even

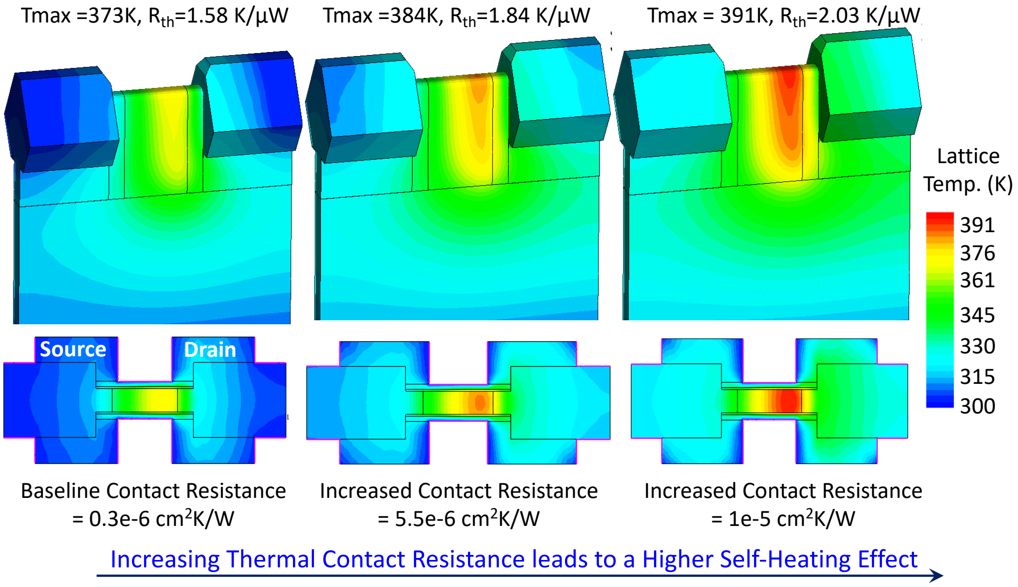

Tmax =373K, R_{th}=1.58 K/µW
Tmax =384K, R_{th}=1.84 K/µW
Tmax = 391K, R_{th}=2.03 K/µW
Lattice Temp. (K)
391
376
361
345
330
315
300
Source
Drain
Baseline Contact Resistance = 0.3e-6 cm^{2}K/W
Increased Contact Resistance = 5.5e-6 cm^{2}K/W
Increased Contact Resistance = 1e-5 cm^{2}K/W
Increasing Thermal Contact Resistance leads to a Higher Self-Heating Effect

Fig. 5: Multi-physics simulations in Synopsys Sentaurus TCAD to accurately analyze the impact of SH in the 14nm FinFET (n-type) devices. As shown, an increase in the contact resistance between the drain-side semiconductor and the metal contact leads to an elevated impact of SH effects due to larger R_{th}. Therefore, such a parameter can be exploited (e.g., by the foundry) as a knob at the design time to tune how much SH should the transistor exhibit later during operation. The larger the SHE, the higher the aging effects and hence the earlier a certain level of degradation can be reached (details in Fig. 6).

in 10 years of operation in the absence of SH, is reached by around 0.41 years. Further, in the presence of SH, a ΔV_{th} of 40 mV can be achieved by merely 2 days. This demonstrates the strong ability of SH to accelerate transistor aging.

C. Methodology to Achieve Desired ΔV_{th}

As will be shown in Sec. III, the proposed HT requires two levels (+40 mV and +80 mV) of SH-assisted ΔV_{th} rise in different transistors of the payload gate. Further, for a foundry-based attacker to be able to clearly define a trigger time (after which the payload is activated with high probability), the time taken for achieving these two levels of ΔV_{th} must coincide. This can be realized by properly tuning the individual transistor parameters like doping and contact resistance.

We demonstrate such a methodology by adjusting the payload transistors' thermal resistance (R_{th}), which is a parameter that can be tuned by the foundry during design time. By setting the appropriate R_{th} for the two different transistor flavors, we can ensure that they achieve +40 mV and +80 mV ΔV_{th}, respectively, at the same time. As indicated, this intersection gives us the trigger time for the HT (Sec. III).

In practice, R_{th} can be effectively changed by increasing the doping concentration or by increasing the extension region length in the transistor as demonstrated in [28]. In addition, tuning the the contact resistance between the drain-side semiconductor and the metal contact is another knob to control R_{th}, because it directly impacts the ability of the transistor to dissipate the SH-induced heat. To investigate this, we employ multi-physics simulations using Synopsys Sentaurus Technology CAD (TCAD) tool flows to accurately analyze the impact of SH in 14nm FinFET (n-type) devices. The baseline device has been calibrated against 14nm measurement data. As shown in Fig. 5, an increase in the contact resistance between drain-side semiconductor and metal contact leads to elevated impact of SH effects due to the larger R_{th}.

Figure 6 highlights a few examples of R_{th} tuning to achieve different trigger times. As demonstrated in Fig. 6, different sets of R_{th} can provide us with the required synchronized ΔV_{th} degradation set of (40mV, 80mV) *at different points of time* such as 10^7 seconds (Figure 6(a)), 5×10^7 seconds (Figure 6(b)), and 10^8 seconds (Figure 6(c)); these times range from around 3.8 months to 3 years, respectively.

III. Construction and Working of Proposed Trojan

A. Self-Heating as a Stealthy Trojan Trigger

We leverage the SH mechanism, described in Sec. II, to cause accelerated aging and deterioration in selected transistors, resulting in functional changes to the original circuit intended by the malicious designer. For this purpose, without loss of generality, we assume threshold-voltage-dependent gates as, e.g., demonstrated in [16].

Such an attack is carried out as follows. Note that, in this work, we consider an SH-prone reconfigurable payload with AND/OR transformation for simplicity.

1) First, the malicious attacker in the foundry modifies the design files obtained from the design house, to add the required threshold-voltage-dependent reconfigurable gates in the layout to be fabricated. The basic premise of these reconfigurable gates is that they exhibit different functional behaviors at different threshold-voltages. For instance, a particular gate might implement AND or OR, depending on the threshold-voltage of its internal transistors. This is illustrated in Fig. 7(a).
2) Recall from Sec. II that the SH mechanism, in the long run, accelerates aging and increases the threshold-

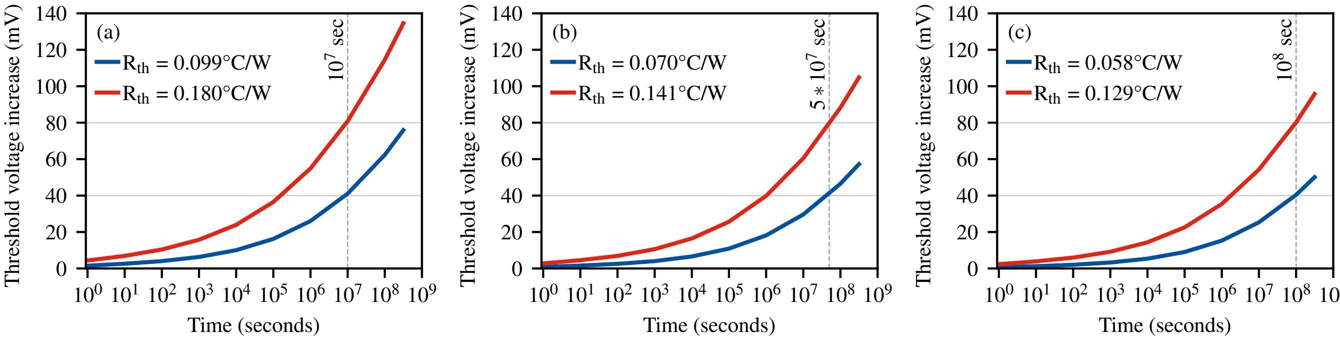


Fig. 6: The thermal resistance of the transistor, which depends on materials and channel doping, can be tuned (*at the design time*) to control later SH effects *at the run-time*. A larger thermal resistance (R_{th}) results in a higher SH-induced temperature and hence a larger aging-induced degradation (ΔV_{th}). Different sets of R_{th} can provide us with the required synchronized ΔV_{th} degradation set of (40mV, 80mV) at different points of time such as (a) 10^7 seconds, (b) 5×10^7 seconds, and (c) 10^8 seconds; these times ranges from around 3.8 months to 3 years, respectively.

voltage by promoting the build-up of defects. We utilize these long-term effects of SH to realize the requisite threshold-voltage change needed for activating the functional changes in the embedded reconfigurable Trojan. As shown in the scheme highlighted in Fig. 7(a), the threshold-voltage increase due to accrued SH effects modifies the gate functionality from AND to OR.

3) Here, the trigger is the threshold-voltage modification caused by SH effects, and the payload is implemented directly via the reconfigurable gate as it changes its behavior depending on the said threshold-voltage. This behavioral change is shown in Fig. 7(b).

B. *Payload Configurations*

Next, we discuss the various configurations to achieve this threshold-voltage dependent reconfigurable payload in the foundry. We use the 7nm FinFET predictive process design kit ASAP7 [29] for our simulations and analyses. We assume that the attacker in the foundry has access to all the standard cells used for fabrication, i.e., high (HVT), regular (RVT), and low (LVT) threshold-voltage cells. He/she can employ techniques like metal work function engineering and doping to achieve the required new threshold-voltage levels for the payload (Sec. II-C).

1) Baseline RVT:

The original NMOS/PMOS RVT levels for ASAP7 at typical process corner, 25°C are 170 mV/-160 mV, respectively. To implement the payload reconfiguration shown in Fig. 7(a), the attacker needs to create three new flavors of transistors that are different from the standard cells provided by the foundry, with V_{th} of ±180 mV, ±140 mV and ±100 mV, for NMOS and PMOS, respectively. These new V_{th} levels ensure an output voltage swing of $\sim$ 20 mV (see Fig. 7(b) AND/OR).

We note here that the resulting 20 mV output swing can be restored to full swing with a simple differential amplifier-based comparator configuration. This implies low power and delay overheads for the post-processing, and hence lower chance of detection. For our analysis, we consider the optimized 7nm FinFET comparator in [30], which operates at ~ 8 μW power and ~ 35 ps delay. The reconfigurable AND/OR payload in baseline RVT configuration itself incurs overheads of ~ 8.71 μW and ~ 4.55 ps over a regular AND gate. Hence, the total power-performance (PP) overheads of the proposed HT payload are ~ 16.71 μW and ~ 39.55 ps.

Assuming that the attacker starts with one type of standard cell, i.e. RVT, he/she would need to engineer the appropriate amounts of ΔV_{th} shifts in the corresponding transistors to obtain the new desired V_{th} levels. For instance, for NMOS, starting with the default RVT level of 170 mV, a ΔV_{th} of (i) $+10$ mV is required to reach the new V_{th} level of 180 mV, (ii) -30 mV is required to reach 140 mV, and (iii) -70 mV is required to reach 100 mV. Similarly, for PMOS devices, the requisite ΔV_{th} shifts to obtain the new V_{th} levels are -20 mV, $+20$ mV, and $+60$ mV, respectively. In this case, the attacker can leverage a combination of metal work function engineering and doping to achieve the positive and negative ΔV_{th} shifts.

2) Baseline LVT:

Now assume that the attacker uses LVT cells as baseline to create new V_{th} levels. Here, the original NMOS/PMOS LVT levels are ±100 mV, respectively. To obtain the new HVT, RVT, and LVT levels of ±180 mV, ±140 mV, and ±100 mV for the payload, the required ΔV_{th} shifts are ±80 mV, ±40 mV, and 0, respectively. In this case, the increments from the baseline ±100 mV LVT are monotonic in nature and easy to engineer, but the small output voltage swing (< 10 mV) requires more complex amplifier/restore circuitry, possibly inducing a larger footprint on PP overheads and thus has a higher risk for detection. Hence, the foundry-based attacker would prefer to start with RVT as baseline to tune the new V_{th} levels required for the HT.

3) Effect of Fin Number:

In general, a larger number fins enhances SH effects and shortens the trigger time after which the payload will be activated. Hence, the fin number is an effective knob for the attacker to set the required amount of trigger time. Recall from Fig. 3 that the fin number is directly proportional to the channel temperature rise, and hence inversely proportional to the time taken to achieve sufficient V_{th} shift (under otherwise identical conditions).

Thus, for the AND/OR circuit in Fig. 7(a), the attacker could hope to achieve the different degrees of V_{th} shift in the

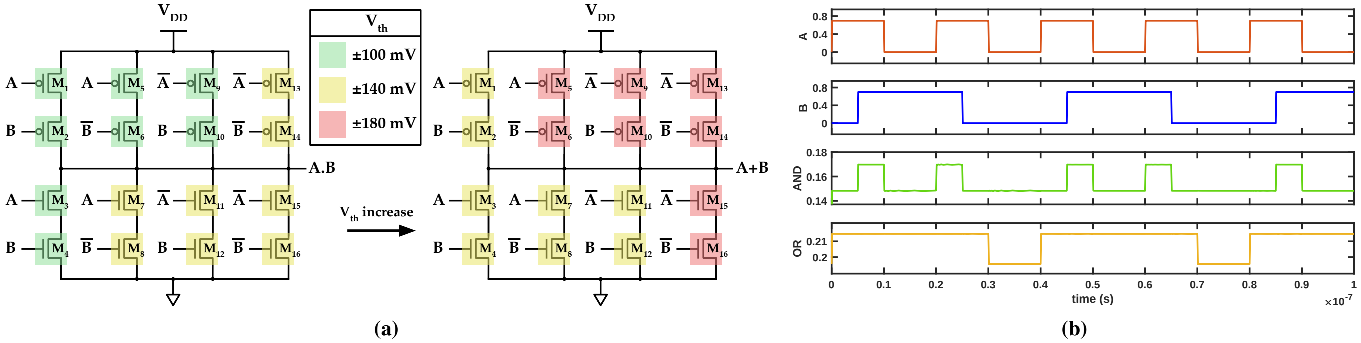


Fig. 7: (a) Threshold-voltage-dependent, reconfigurable gate implementing AND/OR functionalities [16]. The SH-induced threshold-voltage change, as outlined in the figure, transforms the gate from AND to OR. (b) Corresponding output waveforms from SPICE simulations. Supply voltage is 0.7 V.

different transistors (see Table II) by utilizing different number of transistor fins. However, such a differential fin configuration changes the drive current through the transistors and modifies the gate functionality itself, i.e. the transformation is no longer AND ⇒ OR. Hence, the attacker can only increase the fin number consistently across all transistors, to hasten the SH-assisted aging and V_{th} shift uniformly, which will still aid the attacker in accelerating the Trojan activation. As mentioned before, the differential ΔV_{th} in Table II can be achieved by using different metal work functions and doping levels for the different transistors. Also as indicated, the attacker could equalize the trigger time for the two cases, i.e., (i) $\Delta V_{\text{th}} = +40$ mV in some FinFETs and (ii) $\Delta V_{\text{th}} = +80$ mV in other FinFETs, again by appropriately tuning the device doping and metal contact resistance.

C. Resilience against Functional Testing

To ensure evasion from test pattern-based functional testing, an attacker residing in the foundry can determine the test patterns for maximum test coverage for the original design. Next, using these test patterns on an IC injected with the HT, he/she can can ensure that the payload does not get activated during the testing phase. Recall from Sec. II-C, Fig. 6(a) that the trigger time (after which the payload is activated) is designed attacker as 3.8 months; this is well beyond the duration for which the IC is kept operational at the test facility.

Note that specific test data can escalate the ON time for the payload gates, by stimulating the particular nets and fanin cone more frequently. This can, in turn, expedite the SH-assisted aging process in those HT transistors. However, with such a large trigger time buffer, any instances of involuntary HT activation during testing are most likely avoided.

We confirm this by applying 100 random input patterns on selected ITC-99 benchmarks that are injected with our HT payload, to emulate various frequencies of the HT-gate stimulation. That is, we create a testbench for each ITC-99 benchmark and simulate it on Synopsys VCS to capture the payload net values when 100 random input patterns are applied. We find that the payload remains unactivated.

TABLE II: Transistor threshold-voltage shifts required for the AND ⇒ OR reconfiguration in Fig. 7.

Transistor	Initial V_{th}	Final V_{th}	ΔV_{th}
M_1, M_2, M_3, M_4	±100 mV	±140 mV	±40 mV
M_5, M_6, M_9, M_{10}	±100 mV	±180 mV	±80 mV
M_7, M_8, M_{11}, M_{12}	±100 mV	±100 mV	0 mV
M_{13}, M_{14}, M_{15}, M_{16}	±140 mV	±180 mV	±40 mV

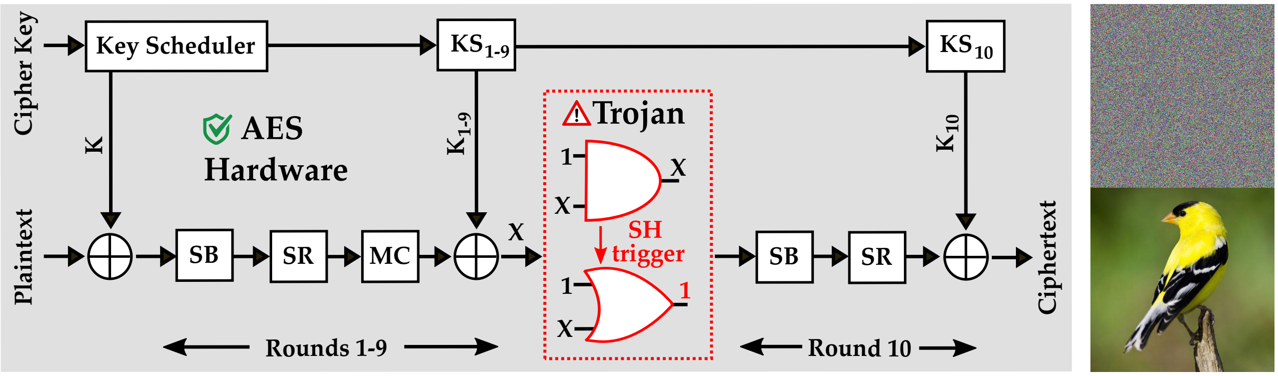
IV. Attack Vectors and Results

A. Chosen-Plaintext Attack on AES

As a proof of concept for the proposed HT, we present a case study on leaking the secret key in a pipelined AES benchmark. Fig. 8(a) highlights the pipelined AES architecture, which consists of 10 rounds. The composition of these rounds is as follows. The first nine rounds are identical and comprise of the SubBytes (SB), ShiftRows (SR), MixColumns (MC), and AddRoundKey (XOR) operations. The tenth round differs in the absence of the MC stage. A key-scheduler module generates the key for each round using the main AES key, which ensures the uniqueness of keys in subsequent rounds. It is important to note that the pipelined nature of the selected AES circuit results in the complete corruption of the ciphertext even when a single bit of the intermediate, round-wise processed text is adversarially modified.

For the attack to work, the foundry-based adversary has to first identify the ideal location in the AES circuit to insert the payload gate. Since the foundry has details of the gate-level netlist to be fabricated, the attacker is readily able to gain access to this netlist, and can determine the implementation of the pipelined AES. Note that, in this architecture, the first nine rounds are pipelined but the last round is excluded from the pipeline. Hence, he/she can readily pinpoint the beginning of the 10th round as the optimal location for injecting the payload [31]; this is also highlighted in Fig. 8(a).

For the Trojan payload, we (acting as the foundry-based adversaries) utilize the reconfigurable gate shown in Fig. 7(a), which functions as AND initially and then reconfigures to OR once the SH-induced V_{th} modulation is complete. After verifying the gate-level AND ⇒ OR transformation from SPICE simulations, we model the same transformation behaviorally in the Verilog RTL model to emulate the Trojan payload. The chosen plaintext ("1" in this case) is passed



(a) **(b)**

Fig. 8: (a) The SH-triggered Trojan is inserted before the 10th round of a pipelined AES architecture [31]. The functional transformation of the payload gate from AND to OR causes a *stuck-at-1*, under the assumption that the corresponding bit of the processed text is also '1', which enables the chosen-plaintext attack. (b) Top: image encrypted with key from 128-bit AES, bottom: decrypted image using the key recovered via the SH Trojan-assisted chosen-plaintext attack.

Algorithm 1: Algorithm for leaking key using chosen plaintext attack on pipelined AES circuit.

```
Input: Ciphertext ($C$)
Output: Key ($Key$)

$K_n$ // $n^{th}$ round key
$\{W_{n\_3}, W_{n\_2}, W_{n\_1}, W_{n\_0}\}$ // Key $k_n$ divided into four 32-bit
  words
$SubByte$ // SubBytes block
$ShiftReg$ // Shift register block
$Rotation$ // Rotation in the key expansion block
$RConst$ // Round constant in key expansion block
$TP$ // Trojan pattern = all zeroes

$K_{10}$ = $\{W_{10\_3}, W_{10\_2}, W_{10\_1}, W_{10\_0}\}$ = ShiftReg(SubByte(TP))
  ⊕ C;
for $i \leftarrow$ 9 to 0 do
    $W_{i\_3}$ = $W_{(i+1)\_3} \oplus W_{(i+1)\_2}$;
    $W_{i\_2}$ = $W_{(i+1)\_2} \oplus W_{(i+1)\_1}$;
    $W_{i\_1}$ = $W_{(i+1)\_1} \oplus W_{(i+1)\_0}$;
    $W_{i\_0}$ = $W_{(i+1)\_0} \oplus SB(Rotation(W_{i\_3})) \oplus RConst$;

$Key$ = $\{W_{0\_3}, W_{0\_2}, W_{0\_1}, W_{0\_0}\}$;
```

to the final round through a stuck-at-1 fault created by the transformation AND ⇒ OR. After the payload is triggered and the functional reconfiguration occurs, Algorithm 1 is used to enact the chosen-plaintext attack and leak all the 128 bits of the AES encryption key. To visually represent this attack, we encrypt a sample image with 128-bit AES (Fig. 8(b, top)) and deduce the secret key using the above chosen-plaintext attack. The obtained key is then used to decrypt the encrypted image and obtain the plaintext image shown in Fig. 8(b, bottom).

Note that the AES circuit is obtained from the OpenCores repository [32]. We synthesize a 128-bit pipelined version of the AES circuit using the ASAP7 FinFET library. We quantify the area and power overheads of the payload and its peripherals as 1.43% and 5.44%, respectively (Table III). Note that, after quantifying the power and delay metrics of the payload gate from the SPICE models, we utilize the same numbers for all HT instances in the pipelined AES simulation for uniformity. It is also important to note that the overheads for this proof-of-concept study can be well reduced for various scenarios, like amortization for larger designs or more careful integration of the HT into the netlist instead of plain addition of logic.

TABLE III: Area and power overheads for the HT payloads injected in the pipelined AES circuit. The additional cells in the Trojan-infected AES circuit correspond to 128 reconfigurable payload gates and 640 gates for the comparators. The area and power of one payload gate is 0.35 μm^2 and 8.72 μW, respectively. The comparators, consuming a power of ~8 μW, are assumed to have a footprint of 1 μm^2 each.

Circuit	Area (cells)	Area (μm^2)	Power (mW)
AES	121,268	12,032.10	39.33
AES_Trojan	122,036	12,204.9	41.47
Overhead	**768**	**1.43%**	**5.44%**

Further, we generate 500 random input patterns for the original AES circuit, which result in identical, genuine responses from the Trojan-infected circuit during testing, since the trigger time for the SH-induced V_{th} modulation is set as 3.8 months. For this experiment, we create a testbench for the Trojan-infected AES circuit and simulate it on Synopsys VCS to capture the payload net values when 500 random input patterns are applied.

B. Output Corruption for Gaussian Blur Filter

For the next case study, we consider a Gaussian blur filter available as intellectual property (IP) module, which performs Gaussian smoothing of the input image to reduce white noise. The Gaussian smoothing operation can be described by the Gaussian function:

$$G(x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{x^2}{2\sigma^2}} \tag{3}$$

where σ is the standard deviation and x is distance from the origin in one dimension.

To construct the Gaussian blur filter IP, we leverage the 32-bit floating point multiplier in [33]. We embed the payload in the multiplier, as opposed to the other components of the filter, since a corrupted multiplier output produces a large deviation from the expected output image. Note that the chosen multiplier is specifically the one used for normalizing the pixels of the original image. We observe that the corruption

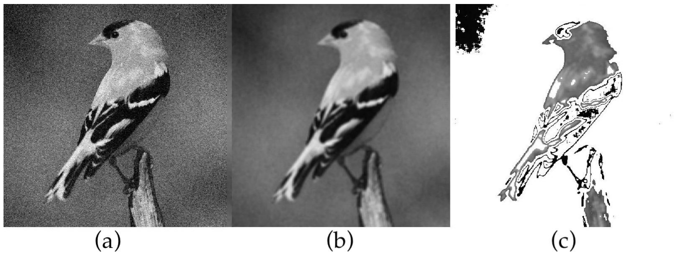


Fig. 9: Output corruption due to HT-infected multiplier in a Gaussian blur filter IP. (a) Original image with white noise. (b) Correct Gaussian blur filtered image. (c) HT-infected image.

is reproducible, wherein the error obtained from payload activation is repeated for identical input patterns.

We highlight the effects of the activated payload on the filter in Fig. 9. The input image (Fig. 9(a)) is expected to look like Fig. 9(b) after the Gaussian smoothing. However, the actual output image obtained resembles Fig. 9(c), due to the HT-infected multiplier. This is because the computation of each pixel is done via the corrupted multiplier; hence, the output image is distorted, rather than displaying a variation in the σ (degree of Gaussian blurring). The corrupted image showcases both positive and negative deviation in pixel intensities with respect to the correct multiplier output, resulting in a non-uniform contrast.

V. Possible Countermeasures

In this section, we discuss possible countermeasures against the proposed SH-based HT and related limitations.

A. Optical Inspection & Image Processing-based Detection

This countermeasure is generic and not limited to our proposed kind of HT. Among others, rapid scanning electron microscopy (SEM) can be used to image ICs [34]. After preparing the IC by depackaging and etching, such techniques are employed to acquire highly magnified images of all parts of the IC and then compare them, through image processing algorithm, with a golden reference (i.e., the design files). Hence, any malicious gate modification, substitution, removal or addition can be detected. However, such techniques may be cost- and time-intensive if applied to larger sample sizes of ICs. More concerning, such imaging-based detection requires destruction of the IC samples and, thus, becomes impractical when to be applied for a large number of ICs. Also, the untrusted foundry may utilize different masks, original versus infected, for different IC batches [35].

B. Neural Network & Machine Learning-based Detection

Recently, machine learning (ML)-aided HT detection has gained traction since such techniques do not require a golden reference IC. For instance, in [36], [37], a hierarchical temporal memory (HTM)-based neural network (NN) uses self-referencing for golden IC-free HT detection. There, the training dataset is collected and features are extracted from the side-channel responses of (i) an HT-inactive IC during the testing phase and (ii) a post-HT-triggered IC. The NN has to learn from both HT-inactive and HT-triggered responses to eliminate false positives/negatives. Hence, the assumption of such techniques is that they can obtain an IC instance with the HT triggered. For the proposed SH-based HT, however, recall that the trigger time can be set appropriately far away in the future. Further, without knowing the payload transistor doping and metal work function, the exact trigger time set by the attacker cannot be properly estimated. Thus, such detection schemes are challenged by our proposed HT.

C. Statistical Power Analysis-based Detection

The power overheads for the AES Trojan example with 128 payload gates in Sec. IV-A, Table III, are $\sim 5\%$ which may blend within process variations. Recall that these overheads would become amortized for larger designs. Still, for malicious applications requiring larger numbers of payload instances, thereby incurring larger overheads, techniques like statistical power analysis [38] might be able to detect the insertion of the proposed HT. Note that more traditional techniques like statistical test pattern generation, leveraging excitation of rare logic conditions at internal nodes to trigger the inserted HT during logic testing [39], will still likely fail if one tailors the proposed HT for a longer trigger time.

D. Voltage Scaling to Mitigate Self-Heating

The trigger time set by the foundry-based attacker assumes a constant supply voltage for the reconfigurable payload gates. Scaling down the supply voltage can also slow down the SH-induced aging effects in the payload transistors and, hence, push back the time until the HT trigger gets activated, delaying the functional transformation expected by the attacker.

VI. Conclusion

Self-heating (SH) in advanced technology nodes is a critical issue, which affects the performance and reliability of modern ICs by degrading the electrical characteristics of transistors. Important parameters like the transistor threshold voltage and carrier mobility can be shifted over time due to the increased thermal resistance and smaller thermal capacitance in confined transistor geometries like FinFETs.

This is the first work to explore the ramifications of SH-assisted accelerated transistor aging in the context of hardware security, especially as a novel vulnerability that enables a foundry-based attacker to inject a stealthy hardware Trojan (HT), which can bypass functional testing.

In this work, we first conduct a comprehensive physics-based modeling and analysis of the SH phenomenon and its effect on the threshold voltage under various conditions. More specifically, using accurate multi-physics simulations in commercial TCAD tool flows, we demonstrate how the contact resistance can be used to tune, at design time, the thermal properties of transistors, thereby quantifying the SH effects that can develop later on at runtime. We then build upon this analysis to design a threshold-voltage-based reconfigurable HT payload, which can be inserted in the target circuit with minimal overheads to enact a variety of attack vectors.

Acknowledgement

The authors would like to thank Ramesh Karri from NYU for the early discussion. The authors are also thankful for the valuable support from Paul R. Genssler, Simon Thomann, and Victor van Santen from the Chair of Semiconductor Test and Reliability (STAR) as well as Om Prakash for the provided analysis in transistor self-heating, SPICE/TCAD simulations, technology calibration, and transistor aging evaluation.

References

[1] D. Nagy, G. Indalecio, A. J. Garcia-Loureiro, M. A. Elmessary, K. Kalna, and N. Seoane, "FinFET versus gate-all-around nanowire FET: performance, scaling, and variability," *IEEE Journal of the Electron Devices Society*, vol. 6, pp. 332–340, 2018.

[2] D. Jang *et al.*, "Device exploration of nanosheet transistors for sub-7-nm technology node," *IEEE Transactions on Electron Devices*, vol. 64, no. 6, pp. 2707–2713, 2017.

[3] Y.-J. Lee, P. Morrow, and S. K. Lim, "Ultra high density logic designs using transistor-level monolithic 3D integration," in *2012 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*. IEEE, 2012, pp. 539–546.

[4] C. Prasad, S. Ramey, and L. Jiang, "Self-heating in advanced CMOS technologies," in *2017 IEEE International Reliability Physics Symposium (IRPS)*. IEEE, 2017, pp. 6A–4.

[5] O. Prakash, C. K. Dabhi, Y. S. Chauhan, and H. Amrouch, "Transistor self-heating: The rising challenge for semiconductor testing," in *2021 IEEE 39th VLSI Test Symposium (VTS)*. IEEE, 2021, pp. 1–7.

[6] Y. Zhao and Y. Qu, "Impact of self-heating effect on transistor characterization and reliability issues in sub-10 nm technology nodes," *IEEE Journal of the Electron Devices Society*, vol. 7, pp. 829–836, 2019.

[7] V. M. van Santen, P. R. Genssler, O. Prakash, S. Thomann, J. Henkel, and H. Amrouch, "Impact of self-heating on performance, power and reliability in FinFET technology," in *2020 25th Asia and South Pacific Design Automation Conference (ASP-DAC)*. IEEE, 2020, pp. 68–73.

[8] W. Ahn, S. Shin, C. Jiang, H. Jiang, M. Wahab, and M. Alam, "Integrated modeling of Self-heating of confined geometry (FinFET, NWFET, and NSHFET) transistors and its implications for the reliability of sub-20nm modern integrated circuits," *Microelectronics Reliability*, vol. 81, pp. 262 – 273, 2018.

[9] V. M. Van Santen, H. Amrouch, P. Kumari, and J. Henkel, "On the workload dependence of self-heating in FinFET circuits," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 67, no. 10, pp. 1949–1953, 2019.

[10] Y. Bi *et al.*, "Emerging technology-based design of primitives for hardware security," *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, vol. 13, no. 1, pp. 1–19, 2016.

[11] S. Patnaik, N. Rangarajan, J. Knechtel, O. Sinanoglu, and S. Rakheja, "Advancing hardware security using polymorphic and stochastic spin-Hall effect devices," in *2018 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE, 2018, pp. 97–102.

[12] N. Rangarajan, S. Patnaik, J. Knechtel, R. Karri, O. Sinanoglu, and S. Rakheja, "Opening the doors to dynamic camouflaging: Harnessing the power of polymorphic devices," *IEEE Transactions on Emerging Topics in Computing*, 2020.

[13] N. Limaye, N. Rangarajan, S. Patnaik, O. Sinanoglu, and K. Basu, "Polyworm: Leveraging polymorphic behavior to implant hardware trojans," *IEEE Transactions on Emerging Topics in Computing*, no. 01, pp. 1–1, 2021.

[14] I. R. Nirmala, D. Vontela, S. Ghosh, and A. Iyengar, "A novel threshold voltage defined switch for circuit camouflaging," in *2016 21th IEEE European Test Symposium (ETS)*. IEEE, 2016, pp. 1–2.

[15] B. Erbagci, C. Erbagci, N. E. C. Akkaya, and K. Mai, "A secure camouflaged threshold voltage defined logic family," in *2016 IEEE International symposium on hardware oriented security and trust (HOST)*. IEEE, 2016, pp. 229–235.

[16] V. S. Rathor, B. Garg, and G. Sharma, "New light weight threshold voltage defined camouflaged gates for trustworthy designs," *Journal of Electronic Testing*, vol. 33, no. 5, pp. 657–668, 2017.

[17] J. Lienig *et al.*, "Toward security closure in the face of reliability effects ICCAD special session paper," in *2021 IEEE/ACM International Conference On Computer Aided Design (ICCAD)*, 2021, pp. 1–9.

[18] J. Knechtel *et al.*, "Security closure of physical layouts ICCAD special session paper," in *2021 IEEE/ACM International Conference On Computer Aided Design (ICCAD)*, 2021, pp. 1–9.

[19] O. Prakash, H. Amrouch, S. Manhas, and J. Henkel, "Impact of NBTI aging on self-heating in nanowire FET," in *2020 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE, 2020, pp. 1514–1519.

[20] S. Salamin, V. M. Van Santen, M. Rapp, J. Henkel, and H. Amrouch, "Minimizing excess timing guard banding under transistor self-heating through biasing at zero-temperature coefficient," *IEEE access*, vol. 9, pp. 30 687–30 697, 2021.

[21] D. Jang *et al.*, "Self-heating on bulk finfet from 14nm down to 7nm node," in *2015 IEEE International Electron Devices Meeting (IEDM)*, 2015, pp. 11.6.1–11.6.4.

[22] O. Prakash, G. Pahwa, C. K. Dabhi, Y. S. Chauhan, and H. Amrouch, "Impact of self-heating on negative-capacitance finfet: Device-circuit interaction," *IEEE Transactions on Electron Devices*, vol. 68, no. 4, pp. 1420–1424, 2021.

[23] R. Wang, J. Zhuge, R. Huang, D.-W. Kim, D. Park, and Y. Wang, "Investigation on self-heating effect in gate-all-around silicon nanowire MOSFETs from top-down approach," *IEEE Electron device letters*, vol. 30, no. 5, pp. 559–561, 2009.

[24] F. Klemme and H. Amrouch, "Scalable machine learning to estimate the impact of aging on circuits under workload dependency," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 69, no. 5, pp. 2142–2155, 2022.

[25] J. P. Duarte *et al.*, "BSIM-CMG: Standard FinFET compact model for advanced circuit design," in *ESSCIRC Conference 2015 - 41st European Solid-State Circuits Conference (ESSCIRC)*, Sep. 2015, pp. 196–201.

[26] D. Jang *et al.*, "Self-heating on bulk FinFET from 14nm down to 7nm node," in *2015 IEEE International Electron Devices Meeting (IEDM)*, Dec 2015, pp. 11.6.1–11.6.4.

[27] S. Makovejev, S. Olsen, and J. Raskin, "RF extraction of self-heating effects in FinFETs," *IEEE Transactions on Electron Devices*, vol. 58, no. 10, pp. 3335–3341, Oct 2011.

[28] U. S. Kumar and V. R. Rao, "A thermal-aware device design considerations for nanoscale SOI and bulk FinFETs," *IEEE Transactions on Electron Devices*, vol. 63, no. 1, pp. 280–287, 2015.

[29] L. T. Clark *et al.*, "ASAP7: A 7-nm finFET predictive process design kit," *Microelectronics Journal*, vol. 53, pp. 105–115, 2016.

[30] T. Masina, K. Rahul, G. MahendraKumar, and S. Yachareni, "Power and performance evaluation of optimized NP-domino comparator in 7nm FinFET for TLBs," in *2021 9th International Electrical Engineering Congress (iEECON)*. IEEE, 2021, pp. 317–320.

[31] A. Jain and U. Guin, "A Novel Tampering Attack on AES Cores with Hardware Trojans," in *International Test Conference in Asia*. IEEE, 2020, pp. 1–6.

[32] "AES-128 encryption," https://opencores.org/projects/aes-128_pipelined_encryption, accessed: 2021-12-12.

[33] "Floating point adder and multiplier," https://opencores.org/projects/fpuvhdl, accessed: 2022-05-12.

[34] F. Courbon, P. Loubet-Moundi, J. J. Fournier, and A. Tria, "A high efficiency hardware trojan detection technique based on fast SEM imaging," in *2015 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE, 2015, pp. 788–793.

[35] S. Bhasin and F. Regazzoni, "A survey on hardware trojan detection techniques," in *2015 IEEE International Symposium on Circuits and Systems (ISCAS)*. IEEE, 2015, pp. 2021–2024.

[36] S. Faezi, R. Yasaei, A. Barua, and M. A. Al Faruque, "Brain-inspired golden chip free hardware trojan detection," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 2697–2708, 2021.

[37] S. Faezi, R. Yasaei, and M. A. Al Faruque, "HTnet: Transfer learning for golden chip-free hardware trojan detection," in *2021 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE, 2021, pp. 1484–1489.

[38] R. Shende and D. D. Ambawade, "A side channel based power analysis technique for hardware trojan detection using statistical learning approach," in *2016 thirteenth international conference on wireless and optical communications networks (WOCN)*. IEEE, 2016, pp. 1–4.

[39] R. S. Chakraborty, F. Wolff, S. Paul, C. Papachristou, and S. Bhunia, "MERO: a statistical approach for hardware trojan detection," in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2009, pp. 396–410.

Nikhil Rangarajan is a Postdoctoral Associate at the Division of Engineering, New York University Abu Dhabi, UAE. He has Ph.D. and M.S. degrees in Electrical Engineering from New York University, NY, USA. Prior to his graduate studies, he completed his Bachelors in Electrical and Electronics Engineering from National Institute of Technology Trichy, India. His research interests include spintronics, nanoelectronics, device physics, and hardware security. His current work aims to explore the security implications of emerging devices-based logic and memory paradigms.

Johann Knechtel is a Research Scientist with New York University Abu Dhabi, United Arab Emirates. He received the M.Sc. degree in Information Systems Engineering (Dipl.-Ing.) and the Ph.D. degree in Computer Engineering (Dr.-Ing., summa cum laude) from TU Dresden, Germany, in 2010 and 2014, respectively. His research interests cover VLSI physical design automation, with particular focus on emerging technologies and hardware security. He was a Postdoctoral Researcher with the Masdar Institute of Science and Technology, Abu Dhabi, from 2015–2016. From 2010 to 2014, he was a Ph.D. Scholar with the DFG Graduate School on "Nano- and Biotechnologies for Packaging of Electronic Systems" at TU Dresden. In 2012, he was a Research Assistant with the Chinese University of Hong Kong, Hong Kong. In 2010, he was a Visiting Research Student with the University of Michigan at Ann Arbor, MI, USA.

Nimisha Limaye received her Ph.D. from the Department of Electrical and Computer Engineering at New York University, USA. Her research interests include hardware security and in particular logic locking, scan locking, and hardware Trojan. She received B.E. in Electronics and Telecommunications Engineering from University of Mumbai, India in 2015 and M.S. in Computer Engineering from New York University, USA in 2017. She has industry experience with Qualcomm and Synopsys. During her Ph.D. she secured third place at CSAW Applied Research Competition, 2020 and CSAW Logic Locking Conquest, 2021.

Ozgur Sinanoglu is a professor of electrical and computer engineering at New York University Abu Dhabi. He obtained his Ph.D. in Computer Science and Engineering from University of California San Diego. He has industry experience at TI, IBM and Qualcomm, and has been with NYU Abu Dhabi since 2010. During his Ph.D. he won the IBM Ph.D. fellowship award twice. He is also the recipient of the best paper awards at IEEE VLSI Test Symposium 2011 and ACM Conference on Computer and Communication Security 2013. Prof. Sinanoglus research interests include design-for-test, design-for-security and design-for-trust for VLSI circuits, where he has more than 200 conference and journal papers, and 20 issued and pending US Patents. Prof. Sinanoglu is the director of the Center for CyberSecurity at NYU Abu Dhabi. His recent research in hardware security and trust is being funded by US National Science Foundation, US Department of Defense, Semiconductor Research Corporation, Intel Corp and Mubadala Technology.

Hussam Amrouch (S'11-M'15) is a Jun.-Professor heading the Chair of Semiconductor Test and Reliability (STAR) within the Computer Science, Electrical Engineering Faculty at the University of Stuttgart as well as a Research Group Leader at the Karlsruhe Institute of Technology (KIT), Germany. He currently serves as Editor at the Nature Scientific Reports Journal. He received his Ph.D. degree with the highest distinction (Summa cum laude) from KIT in 2015. His main research interests are design for reliability and testing from device physics to systems, machine learning for CAD, HW security, approximate computing, and emerging technologies with a special focus on ferroelectric devices. He holds eight HiPEAC Paper Awards and three best paper nominations at top EDA conferences: DAC'16, DAC'17 and DATE'17 for his work on reliability. He has served in the technical program committees of many major EDA conferences such as DAC, ASP-DAC, ICCAD, etc. and as a reviewer in many top journals like Nature Electronics, T-ED, TCAS-I, TVLSI, TCAD, TC, etc. He has around 185 publications (including 74 journals) in multidisciplinary research areas across the entire computing stack, starting from semiconductor physics to circuit design all the way up to computer-aided design and computer architecture. His research in HW security and reliability have been funded by the German Research Foundation (DFG), Advantest Corporation, and the U.S. Office of Naval Research (ONR). ORCID 0000-0002-5649-3102.