Large Delay Analog Trojans: A Silent Fabrication-Time Attack Exploiting Analog Modalities

Tiancheng Yang, *Graduate Student Member, IEEE*, Ankit Mittal, *Graduate Student Member, IEEE*, Yunsi Fei, *Senior Member, IEEE*, and Aatmesh Shrivastava, *Senior Member, IEEE*

***Abstract*— This article presents large delay-based analog Trojan circuits, a new class of analog Trojans that can be interfaced with digital and analog macros to launch fabrication-time hardware attacks. Two different circuit topologies of analog Trojan are presented, which can generate a delayed trigger output after two days and 60 ms, respectively, when implemented in 65-nm CMOS technology. The large delay is achieved using the transistor's gate-oxide leakage current or a diode's reverse saturation current in combination with the Miller capacitance-based circuits. The proposed analog Trojans can operate across multiple on-chip power domains and can be launched without any digital input signal, making their detection challenging. They show very limited variation in side-channel parameters, which makes them harder to detect through side-channel analysis. In addition, the proposed designs have a small area footprint of 55.5 μm^2 and 28 μm^2, respectively, and can be easily concealed on-chip. We also demonstrate an attack launched using these Trojans to construct a "kill-switch" that disables the power management unit of an IC. Process and temperature variations were also investigated to assess their impact on the design. We implemented the thick-oxide gate leakage modeling to study the robustness of the proposed Trojan design. We also present the long-term potential threat of these Trojans where the output trigger signal is generated after an even larger delay.**

***Index Terms*— Analog Trojan, gate-oxide leakage, hardware security, hardware Trojan (HT).**

I. Introduction

CHIP design, which is used to be largely an in-house design activity, has now transformed into a supply chain-based process, where the design involves the integration of third-party IPs, and the manufacturing is outsourced to a handful of foundries. Under such a horizontal business model, fabless [1] design companies are particularly vulnerable to all sorts of malicious hardware Trojan (HT) insertion at design time and manufacturing time. A compromised IP vendor or an adversary integrator can embed Trojans into the design (whether it is a soft IP, a hard IP, or a firm IP). Untrusted foundries for chip fabrication can add extra logic or modify the layout during manufacturing time [2]–[10]. HTs pose a significant risk to military and civilian applications by denying services at critical times, stealthily disrupting operations, or stealing information via backdoors. Some of the unexplained hardware failures in military applications have been attributed to HTs [11]–[13].

HTs can be realized as a digital circuit, analog circuit, or a dopant-induced malware circuit. In dopant-induced HTs, an adversary foundry modifies the doping level of transistors to compromise the digital logic. Researchers induced accelerated aging in transistors by increasing the dopant concentration to lead to early device failure [14]. Another approach shows replacing the $p+$ doping in a pMOS transistor to $n+$ to generate an always high logic irrespective of inputs [4]. However, dopant-level Trojans lack effectiveness in launching hardware attacks as they can be easily identified during chip validation [6]. Digital HTs, on the other hand, are more effective as they can disguise inside the logic layout to evade detection. Design strategies include utilizing do not care states of the logic for trigger [15], counters to realize large count-based trigger [16], and rare input condition-based trigger [17], or exploiting side-channel attack resilient designs using parametric Trojans [18], among other techniques. Digital HTs have been extensively studied, and various strategies for detection and mitigation also exist [8], [10].

Analog Trojans, such as A2 and row-hammer [19], [20], are relatively new and far more stealthy. They are smaller sized and may not rely on inputs for triggering, and their trigger output can be made very/arbitrarily long (a ticking time bomb). Due to their novel nature and incompatibility with the digital design and validation flow, analog Trojans can easily evade detection [19]. Only a few methods to detect analog Trojans have been reported in the literature [21]–[23]. However, they target specific analog Trojans that require a trigger input or incur costs for deprocessing and detection logic.

In this article, we present a new class of analog Trojan circuits that generate extremely large delay trigger output signals, in hours and days, with a small area footprint. The proposed analog Trojan can also operate with or without using any input signal and can be simply triggered through the power-up of a

Manuscript received June 17, 2020; revised September 12, 2020; accepted October 20, 2020. Date of publication November 16, 2020; date of current version December 29, 2020. This work was supported in part by the National Science Foundation under Grant IUCRC—1916762 with the industry support from the Center for Hardware and Embedded Systems Security and Trust (CHEST) and Analog Devices Inc. *(Corresponding author: Ankit Mittal.)*

The authors are with the Department of Electrical and Computer Engineering, Northeastern University, Boston, MA 02115 USA (e-mail: yang.tianch@northeastern.edu; mittal.ank@northeastern.edu; yfei@ece.neu.edu; aatmesh@ece.neu.edu).

Color versions of one or more of the figures in this article are available online at https://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TVLSI.2020.3034878

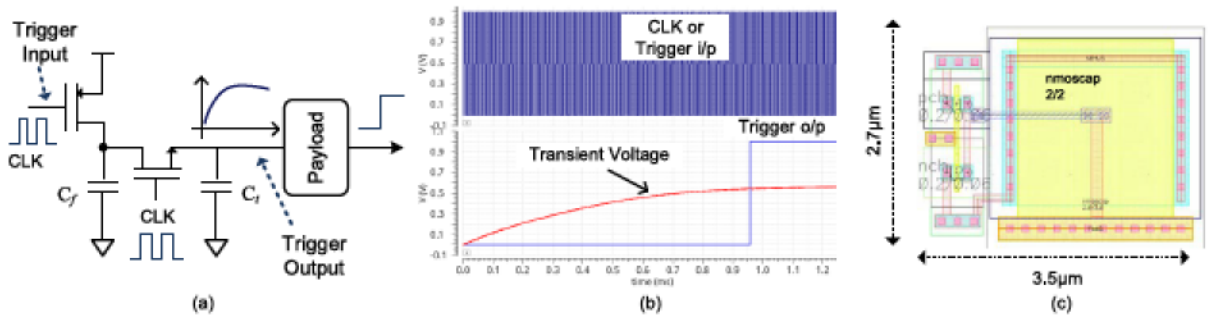

Fig. 1. Circuit architecture, operation, and layout of the A2 Trojan [19]. (a) Circuit architecture of A2 Trojan. (b) Simulation of A2 Trojan. (c) Layout of A2 Trojan in 65-nm CMOS.

chip. Its potential to generate trigger without input and after a very long delay makes it harder to detect using conventional validation methods. The significantly delayed trigger output can be used by an adversary to generate a "kill-switch" on the chip akin to a time bomb to deny services in critical civilian and military applications. This article also presents the construction of such a use case with the proposed Trojans to launch an attack on the power management unit (PMU) of a chip.

II. Background

Analog Trojans are emerging as a stealthier threat than their digital counterparts. They rely on analog conditions or stimulus for their deployment, rather than certain operating state or input conditions. Row-hammer attack in densely packed DRAM manifests through the electromagnetic coupling between adjacent bit cells. The electromagnetic coupling is enabled by making one or more bit cells rapidly active [20], resulting in the charge-leakage of adjacent bit cells and leading to cause faults [24]. Row-hammer has been used to launch different types of cyberattacks, such as unauthorized access of kernel [25], disruption of deep neural networks (DNNs) [26], overtake of a remote server [27], and leakage of cryptographic information using side-channel attack [28]. Other analog mode Trojans have also been demonstrated to cause cache memory leakage [29] and resetting of translation look-aside buffer [30]. Recently reported A2 analog Trojan operates on the principle of switched-capacitor charge transfer. The authors used A2 Trojan to launch a remotely controllable privilege escalation attack on OR1200 processor [19]. The area footprint of A2 Trojan can be made very small, and its trigger output can be made very long, making it extremely stealthy. Researchers have also exploited multiple operating points of nonlinear analog circuits to develop analog Trojans [31].

A. Charge Injection-Based Analog Trojans

A2 Trojan and row-hammer attack are charge injection-based attacks. Fig. 1(a) shows the circuit architecture of A2 Trojan. The trigger circuit is composed of a flying capacitor C_f, a storage capacitor C_t, and two small switches driven by a toggling input (e.g., the clock or a certain bit of some registers), which acts as the trigger input. The payload circuit can be a digital gate. A2 Trojan operates in a dynamic manner to store charges on C_t via charge-sharing by C_f. During each cycle when the clock or input goes low, the capacitor C_f charges up to V_{DD}. When the clock goes high, the stored charge on C_f is shared with C_t. As C_t is comparatively larger than C_f, it will take multiple switching cycles for the voltage on C_t and V_t to rise high. As the voltage rises, a connected digital payload circuit will generate a trigger output. Note that the trigger output is generated at a later time, which can be made large to evade detection during validation. Furthermore, a specifically designed activity mode can have enough switching activity to enable the trigger output. We simulated the A2 Trojan circuit in a 65-nm CMOS process. Fig. 1(b) shows the simulation result. The trigger output signal was generated after 100 s of switching cycles of a low-frequency clock. Row-hammer-based Trojans also operate in a very similar manner. A2 Trojan can be designed using a small area. Our layout of the A2 Trojan circuit consumes less than 10-μm^2 area [see Fig. 1(c)] and is made compatible with the standard cell and filler cell layout, possibly being hidden inside a synthesized digital logic block.

The trigger input for A2 and row-hammer requires a switching input, and its trigger output can be generated within 10 s of μs of input trigger. Trojan detection and prevention methods using these features have been proposed. One method proposes to periodically reset switching signals to prevent A2 deployment [23]. Similarly, exhaustive validation methods where signals can be made to switch for a longer duration can also potentially be used for their detection. Our proposed analog Trojans circuits generate output after a large delay and can also be triggered without any input signal. The absence of trigger input signal renders the test input vectors ineffective, while a very large delay will make detection during IC validation challenging.

III. Large Delay-Based Analog Trojan

Analog delay-based Trojan may not use any digital input signals or generate a long delay once a rare digital event happens. They cannot be easily detected through conventional chip-validation techniques. An adversary can utilize the large delay Trojans to launch different types of attacks.

A. Threat Model

The insertion of HTs is possible at multiple stages of the design cycle. Multiple attack models are possible by inserting HTs at different stages of chip design [32].

1) *Untrusted 3PIP Trojan Model:* Third-party IP (3PIP) providers for analog IPs, such as for BGR, LDO,

and ADCs, among others, may already have the malicious HTs inserted, which can compromise the chip functionality.

2) *Untrusted SoC Developer Trojan Model:* The design and integration of functional IPs in an SoC are done in several stages with scaling complexity requiring design expertise. In such cases, the design work/SoC integration may be outsourced to third-party design houses or contractors. These third-party design houses can act as an adversary (rogue designers) by introducing HTs in the design or during SoC integration.
3) *Untrusted Fab or Fabless Design House Trojan Model:* The foundry, as an adversary, has the access to the GDSII file, the geometrical representation of the design. This allows the adversary to access and assess the design, concealing the proposed analog HTs inside nonfunctional filler cells, decoupling capacitors, or analog designs. The adversary makes the Trojan trigger, a rare scenario that will likely go undetected during a conventional production test.

B. Design Objectives of the Analog Trojan

1) *Functionality:* The proposed Trojan circuit can be used to launch an attack on the critical on-chip infrastructure circuits, such as PMU, oscillators, and ADC, among others. This can easily lead to partial or complete disruption of the design functionality of the chip.
2) *Area:* The layout of the Trojan circuit must be smaller to make it easier to conceal. The lower area is important to make detection difficult even with reverse engineering.
3) *Power Consumption:* To evade detection through side-channel analysis, Trojan should ideally consume zero power. The power consumption of the Trojan must be minimized such that it gets masked by the on-chip power fluctuations.
4) *Trigger Event:* The event that triggers the Trojan must be a rare event or independent of any stimulus, ideally insensitive to the production test patterns.
5) *Timing Impact:* The Trojan circuit must not alter the timing delays on the functional path and leave no signature for traceability. The proposed analog HTs are not in the functional path of the design; hence, it would go undetected by a robust timing analysis.

Fig. 2 shows the circuit architecture of two Trojans based on on-chip current sources that can generate a very large delay output signal. The proposed design techniques use some of the lowest sources of current available on-chip in combination with capacitors to realize large delays. In one topology, we use reverse saturation current of a small on-chip diode [see Fig. 2(a)] to realize a trickle-charge (TC)-based analog Trojan. In another architecture, we use the gate leakage (GL) of thin oxide transistors to realize a GL analog Trojan. These Trojans can be activated simply from power supply to make them independent of digital stimuli needed for activation. They can also use a combination of a rare digital signal and its assertion for a set amount of time to get activated.

Capacitance Enhancement: The two designs draw low current from different circuits while sharing a common design of

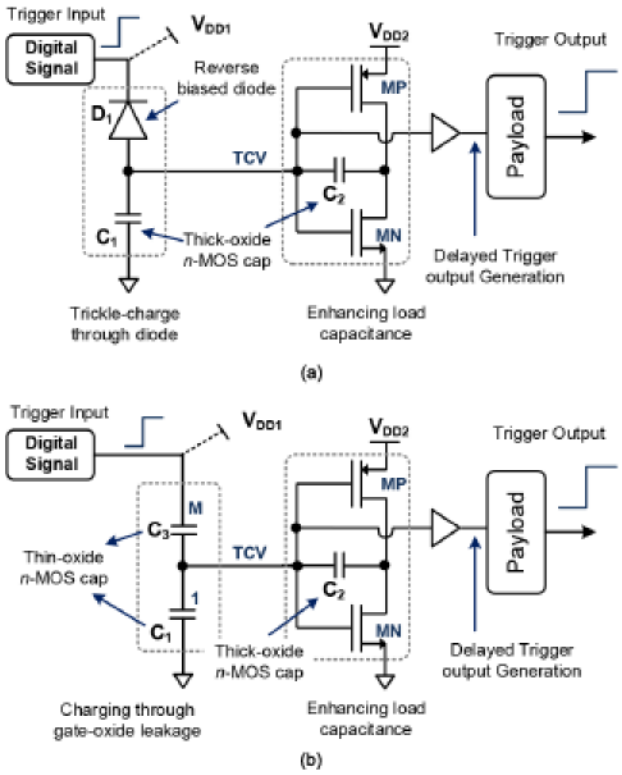

Fig. 2. Circuit architecture of large delay-based analog Trojans. (a) Diode's reverse saturation current-based TC Trojan. (b) Thin-oxide gate leakage-based GL Trojan.

enhancing capacitance, as shown in Fig. 2. The value of the load capacitance that is needed to generate the delayed trigger output signal can be further enhanced using circuit techniques, such as the Miller effect. We used capacitor C_2 in the Miller configuration for both GL and TC Trojans in order to enhance the capacitor seen by the current sources, which will be AC_2 around the transition point of the first inverter where A is the inverter gain given by

$$A = \{g_{mn} + g_{mp}\} \cdot r_{ON} || r_{op} \tag{1}$$

where g_{mn} (g_{mp}) is the transconductance and r_{ON} (r_{op}) is the output resistance of nMOS (pMOS) device. The value of A can vary from 20 to 40 dB (10–100) depending on the design of the inverter. The combination of low-current source level and enhanced capacitance value helps in generating very large delays, and it is well suited for developing large delay-based analog Trojans.

C. Circuit Architecture of TC Trojan

One of the lowest sources of on-chip current can be a reverse-biased diode through its reverse saturation current I_s, which can be used to charge an on-chip capacitor. When charging the capacitor through a low-current value, the leakage of the capacitor also needs to be very small. To ensure extremely low leakage of the on-chip capacitor, a thick-oxide (IO-device) MOS capacitor is used. Fig. 2(a) shows the circuit architecture of the TC Trojan circuit using the reverse-biased diode and thick-oxide nMOS capacitor.

The reverse saturation current density J_s of a silicon pn diode is given by

$$J_s = \frac{qD_p n_i^2}{L_p N_D} + \frac{qD_n n_i^2}{L_n N_A} \quad (2)$$

where D is the diffusion constant, L is the diffusion length, and N_D and N_A are the donor and acceptor impurity concentrations on n and p sides, respectively. On-chip diodes made out of p^+n doping can have the value of J_s in the range of 10^{-12} A/cm^2 [33] at room temperature. The modern device manufacturing process enables extremely small feature sizes. In the 65-nm CMOS process, diodes of size 0.25–0.25 μm can be drawn, which can theoretically realize the I_s values of the order of 10^{-20} A. We carried out the design and simulation of a 65-nm p^+n diode, which gives an I_s value of less than 10^{-18} A (1 aA). The circuit was simulated using a SPICE simulator with a current tolerance of 10^{-25} A. This low-current value can be used to charge a 1-fF capacitor taking 500 s to charge to 0.5 V.

The leakage of the capacitor being charged also becomes an important factor when charging at such low-current values. The advancement of CMOS scaling has resulted in significant GL in thin-oxide devices due to different forms of tunneling. However, thick-oxide devices, available for IO and analog designs, have very low GL values. The GL current density for a 30-Å n-poly gate p-sub-MOS devices is below 10^{-10} A/cm^2 for 1-V gate bias [34]. For thicker oxide and a lower bias voltage of 0.5 V, the current density will be much lower. The GL current for thick-oxide devices is not modeled in SPICE due to their extremely low values. We provide a detailed analysis of TC Trojan design in Section III-C1 when thick-oxide leakage is considered. We used thick-oxide nMOS capacitors that are realized using n-poly gate over n-Well. It has a density of approximately 5 fF/μm^2.

Using the Miller-effect circuit technique discussed earlier, the signal delay can be increased several fold while keeping the area of TC Trojan small. We designed and simulated the TC Trojan circuit in a 65-nm CMOS process where thick-oxide devices are available for IO design. Fig. 3(a) shows the simulation result of the TC Trojan circuit. After V_{DD1} is powered up, the TC voltage (TCV) rises slowly through I_s of the diode. While this rise takes a significant time in itself due to the low value of I_s, the Miller-effect makes it even longer, as shown in Fig. 3(a). The TCV signal takes approximately 170 ks to rise to 0.5 V, and the trigger output signal gets generated. It takes about 170 ks to generate the trigger output, approximately two days after power-up. This delay time is significantly larger than a few seconds of test time that ICs spend on ATE testers [35], [36].

The layout design of TC Trojan is also shown in Fig. 3(b). The area of this design is small, around 7.4 μm × 7.5 μm. TC Trojan is primarily made out of capacitors and can easily hide inside the decoupling capacitor used on-chip for power supplies. The size of the design without the capacitors is approximately 3 μm × 3 μm.

Another advantage of C_2 in the Miller configuration is to make the design more robust against gate-oxide leakage, which is not modeled for thick-oxide capacitors. In case the

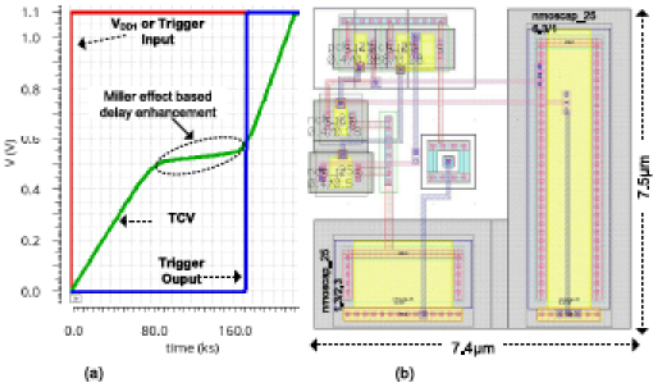

Fig. 3. (a) Simulation result and (b) layout of TC Trojan.

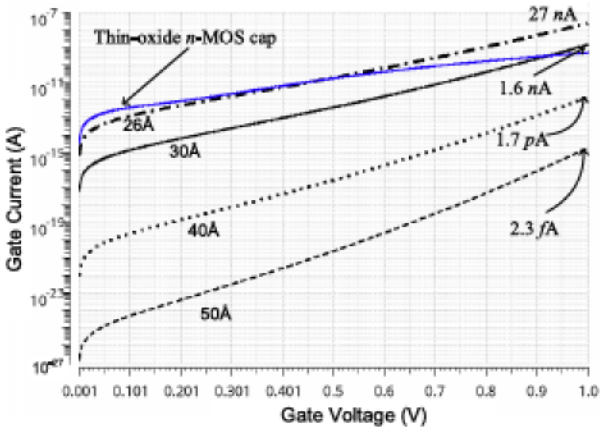

Fig. 4. Modeling of gate-leakage current with gate voltage and oxide thickness (t_{ox}) for an nMOS capacitor ($W = 5$ μm and $L = 1$ μm).

gate-oxide leakage comes out to be comparable to I_s, even then the TCV signal will be charging up through the gate-oxide leakage of C_2. C_2 is chosen to be much larger than C_1. When the voltage drop across C_2 reduces as TCV is charging up, the diode current I_s can still provide trickle charging of TCV realizing the large delay needed for trigger output.

1) Leakage Consideration of Thick Oxide: In this section, we consider the implications of finite GL in thick-oxide devices. The gate-oxide leakage current can be significant for thin-oxide devices, and the leakage current density J_g is given by

$$J_g = A \cdot \left[\frac{t_{oxr}}{t_{ox}}\right]^N \cdot \frac{V_g \cdot V_{aux}}{(t_{ox})^2} \cdot e^{-B.t_{ox}(\alpha - \beta \cdot V_{oxa})(1+\gamma \cdot V_{oxa})} \quad (3)$$

where $A = 4.97232 \times 10^{-7}$ A/V^2, $B = 7.45669 \times 10^{11}(g/F - s^2)^{0.5}$, α, β, γ, t_{oxr}, and t_{ox} are the BSIM4 SPICE model parameters, and N is the fitting parameter [37]. The gate-oxide leakage current (3) is used for modeling GL current in the BSIM4 SPICE model for thin-oxides operating in accumulation region. Note that we operate the nMOS capacitor in the accumulation region. Equation (3) shows the exponential dependence of GL on both oxide thickness and the voltage across it.

2) Modeling of Thick-Oxide Leakage: In Section III-C, we showed the simulation results for the thick-oxide-based design of TC Trojan. Their GL is not modeled in the BSIM4

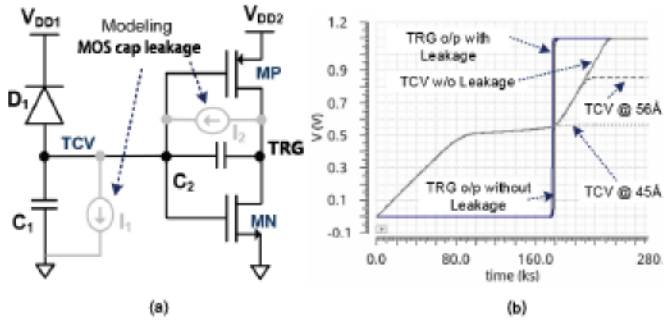

Fig. 5. Impact of finite gate-oxide leakage in TC Trojan delay. (a) Additional current sources to model gate-oxide leakage. (b) Comparison of TC Trojan function in the presence of gate-oxide leakage.

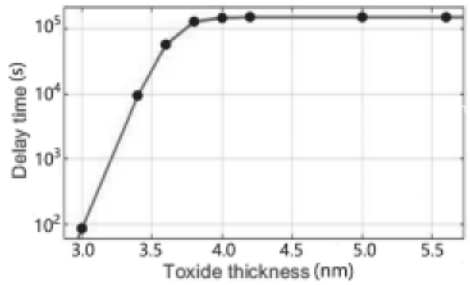

Fig. 6. Variation of TC Trojan trigger delay with t_{ox} using the proposed GL model.

SPICE model. To include the effect of GL current of thick-oxide devices, a behavioral model for GL current based on (3) was developed in Verilog-A. A modified SPICE model for thick gate oxide was simulated and compared with the GL Verilog-A model to ensure the correctness of the model. The effect of the GL of thick oxide is included by varying the gate-oxide thickness (t_{ox}) in the Verilog-A model, as shown in Fig. 4. To verify the accuracy of the Verilog-A model, we also compared our model at 26-Å oxide thickness with SPICE model-based leakage of the 65-nm thin-oxide nMOS capacitor whose gate-leakage is modeled in SPICE. The variation of the SPICE model current is shown by the solid (blue) curve in Fig. 4. Our Verilog-A model shows close agreement with the SPICE model-based gate-leakage in thin oxides.

We used the model of gate-oxide leakage for thick oxide with varying oxide thickness to study the robustness of delay given by the TC Trojan circuit. The model introduces two additional current sources that will appear in the design due to each capacitor, ignoring the GL of M_P and M_N due to their smaller size. Fig. 5(a) shows the additional current I_1 due to C_1 and I_2 due C_2 included in the circuit. Since C_2 is designed to be larger than C_1, I_2 is correspondingly larger than I_1 for the same bias voltage. Initially, TCV is sitting on the ground, and both I_s and I_2 will start charging it. When TCV rises, the value of I_2 will decrease because of the decrease in the voltage across it. Furthermore, as TCV increases, the value of I_1 increases, which effectively reduces the current charging TCV. Fig. 5(b) shows the simulation result for t_{ox} values of 56 (which is the t_{ox} value of thick oxides) and 45 Å for a pessimistic comparison. It shows that TCV charging rate, in the beginning, remains almost constant across both t_{ox} values due to the higher value of I_s. However, as TCV starts increasing, the voltage across C_2 changes and so does the direction of the gate-leakage current, which prevents the voltage to reach the value of V_{DD2}. When the input of the inverter is equal to the output (the threshold voltage), I_2 will go to zero. At this point, I_s will charge TCV, increasing it above the threshold voltage to cause the transition. Note that the attacker will keep the value of I_1 low relative to I_s to ensure the transition of state. While the value of I_2 does not impact the functionality of Trojan, it can make the initial charge-up much faster at lower values of t_{ox}. Fig. 5(b) shows that the trigger is generated after 170 ks. Our analysis shows that a relatively large delay trigger signal can be generated reliably even when correspondingly pessimistic GL of thick oxide is considered in the design.

We simulated the TC trojan circuit with the thick-oxide leakage using the Verilog-A model as discussed earlier. The oxide thickness for our thick-oxide transistors and capacitors is 56 Å. The delay time generated from TC Trojan using this mode is 170 ks, as shown in Fig. 6. The diode leakage current comes out to be relatively higher than the gate-oxide leakage of thick-oxide devices. Our simulations for the proposed design show that the diode leakage current was 0.38 A. Meanwhile, the current from thick-oxide GL current was around 10×10^{-24} A at a 500-mV bias. The simulation results show that the impact of thick oxide leakage on the value of the delay generated is minimal, and the diode leakage is the main factor in charging the capacitor. Fig. 6 shows the change of delay time of TC Trojan when the oxide thickness t_{ox} is varied. If t_{ox} is thicker than 42 Å, the generated delay time has no impact. Leakage current can be ignored with a thick oxide. If the oxide is thinner than 36 Å, the GL will increase rapidly, and the delay time will reduce quickly. The above analysis provides two important design insights. First, the thick-oxide GL does not seem to contribute significantly to the delay of TC Trojan, and the design is robust around the variation of oxide thickness or modeling error. In addition, in cases where GL is still high, for t_{ox} of over 30 Å, the proposed design still generates a very large delay of 10–100 s of ks delay, realizing the central goal of very large delay to evade detection during validation.

3) Other Design Considerations: Since this design is realized using a very low current, we also evaluated its sensitivity to noise generated from the design components. The circuit generated approximately 100 μV of noise on the TCV, which is reduced due to the presence of capacitors showing a low impact on the Trigger signal. We also simulated the circuit for process and temperature variation. Fig. 7(a) shows the simulation of TC Trojan against process variation. It shows a normal distribution with a mean (μ) of 187 ks and a standard deviation (σ) of 43 ks. The circuit shows a strong dependence on temperature due to the variation of I_s on temperature. Fig. 7(b) shows the exponential dependence of trigger generation of TC Trojan on temperature. We also simulated the variation of delay with respect to the power supply. A $\pm$20% variation in power supply results in a $\pm$21% variation in the delay.

Another important feature of analog Trojans, including TC Trojan, is that they can operate across power domains.

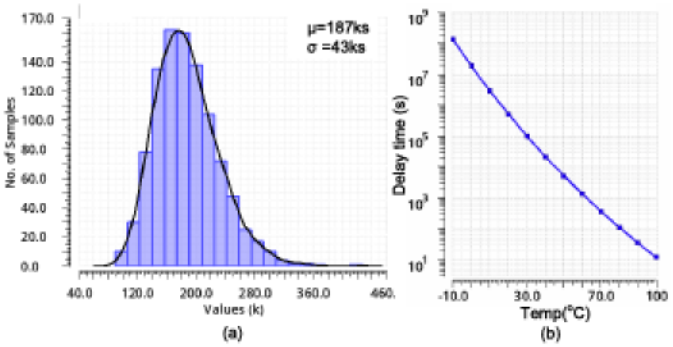

Fig. 7. Simulation of TC Trojan against process and temperature. (a) Process variation of trigger generation. (b) Temperature variation of the trigger.

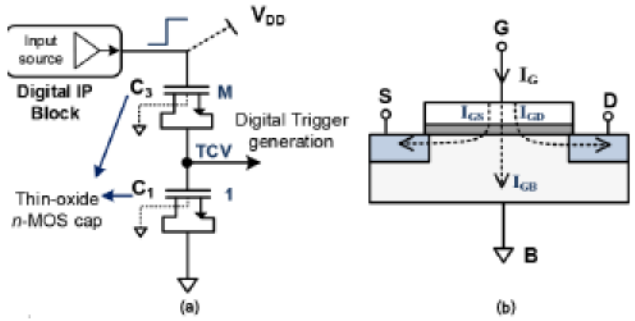

Fig. 8. Gate-leakage-based Trojan signal generation. (a) Capacitor charging in GL Trojan. (b) Gate leakage in MOS device.

The circuit in Fig. 2 shows this feature. The charging of the TCV node is carried out by the current from V_{DD1} or when a digital signal turns on, but its output is connected to a gate operated in V_{DD2}. This feature provides additional stealth to the analog Trojan with its ability to operate across voltage domains. Especially, if a power supply (V_{DD1}) is used as the input signal, the power-up sequencing is important where V_{DD1} rises after V_{DD2}. Since V_{DD2} rises first, any additional charge coupled to TCV net will be discharged through the diode to V_{DD1} having a low impedance to a potentially ground level (when V_{DD1} is not powered). In modern computer and system design, system-level power management often involves multiple power domains using different supplies that are powered ON and OFF to tradeoff between power and performance. These power supplies can be used as targets for the deployment of TC Trojan. For example, the RF power supply used in various mobile applications can be a target as it is typically on only for a short duration to save power. In a rare scenario, this RF power supply can be used for a longer duration. A TC Trojan attached to RF power supply will be mostly not triggered but can be triggered in that rare application scenario and becomes application/operating mode-specific.

In another form of deployment, a rare digital input (e.g., a reserved configuration bit) can also be used as the trigger input for the TC Trojan. For activation, the particular digital signal should remain high for a long time to activate it. Since the delay generated from TC Trojan is very large, the adverse effect due to the signal going high will not be seen during validation. However, an adversary can design the Trojan to evade detection during validation and write a specific software code that can set a digital register to trigger the Trojan in the field. An additional bit generation can be used for a variety of attacks that we discuss in Section IV.

TC Trojan can be deployed with significantly high stealth compared with other fabrication-time HTs. It has a small area, most of which is used by the capacitor, which enables it to be hidden easily, specifically around on-chip decoupling capacitors. The extremely large delay of over 2 days can make it harder to detect with conventional validation methods. Furthermore, it does not require an input signal and can hide on-chip like a ticking time bomb to deny service at a later time when the chip is deployed in the field. We demonstrated the TC Trojan capability using a small capacitor. However, an attacker can make it even stealthier by using a higher capacitor value for C_2. We also simulated the design with a C_2 value of 10 pF, which generates the trigger output after one year. The area needed for this design is 40 μm $\times$ 40 μm, which is high but easily realizable on-chip, particularly around large analog blocks of PMU.

D. Circuit Architecture of GL Trojan

TC Trojan utilizes lower values of a diode's reverse saturation current to realize a delayed trigger signal. Another on-chip source of lower values of current is gate-oxide leakage, particularly in thin-oxide devices. GL Trojans are realized using the thin-oxide GL. Fig. 8(a) shows the realization of delayed trigger output. The trigger voltage TCV is generated using gate-leakage, while the rest of the Trojan circuit remains the same. Two thin-oxide nMOS capacitors, C_1 and C_3, are used for this purpose. C_3 is sized M times bigger than C_1 to ensure that TCV charges above the threshold voltage of the next digital gate.

Gate-oxide leakage current manifests in thin-oxide devices due to various forms of tunneling. The leakage current is composed of the gate–source tunneling current I_{GS}, the gate–drain tunneling current I_{GD}, and the gate-bulk tunneling current I_{GB}. In the case of C_1, gate, source, and bulk are all tied together, while in the case of C_2, drain and source are tied together, while bulk remains at the ground. Consequently, the voltage division by the two capacitors is not equal with part of the GL current for C_3 that does not flow toward TCV. However, the size of C_3 is made larger to keep the settling voltage of TCV higher to cross the threshold voltage of the next digital gate.

We simulated and completed the physical design of GL Trojan. Fig. 9(a) shows the simulation results. The trigger output is generated 60 ms after the input trigger signal is provided. The trigger input needs to remain asserted for the entire 60 ms. Although the delay from GL Trojan is significantly lower than the TC Trojan, it still generates a large delay, making it harder to identify during validation. It takes 28 μm^2 of area. Fig. 9(b) shows the layout of the GL Trojan. We also simulated the process and temperature variation of the delay generated by GL Trojan, as shown in Fig. 10. The mean delay (μ) of GL Trojan is 61 ms with a standard deviation (σ) of 30 ms. The temperature variation of the GL Trojan is relatively low. This is primarily because GL Trojan is based

TABLE I
COMPARISON OF PROPOSED ANALOG TROJANS WITH OTHER HTS

	A2 [19]	[38]	[29]	HarT-Bleed [30]	TC (This Work)	GL (This Work)
Technology	65nm	NA	22nm-PTM	22nm-PTM	65nm	65nm
Type	Analog	Digital	Digital	Digital	Analog	Analog
Attack Type	Privilege Esc.	Privilege Esc.	Memory Attack	Memory Attack	Kill-Switch	Kill-Switch
Input	Sw. signals	Logic combination	Sw. signals	Sw. signals	None/Rare Input	None/Rare Input
Area	$13\mu m^2$	$80\mu m^2$	$0.0099\mu m^2$	$43\mu m^2$	$55.5\mu m^2$	$28\mu m^2$
Power	$500/5.3nW$	-	$0.6\mu W$	$4.3\mu W$	$10nW^*$	$900nW^{**}$
Trigger Output Delay	$5/1\mu s$	-	-	$18\mu s$	2-days	60ms

*Power measured after 1-hour of input trigger.
**Power measured after 10ms of input trigger.

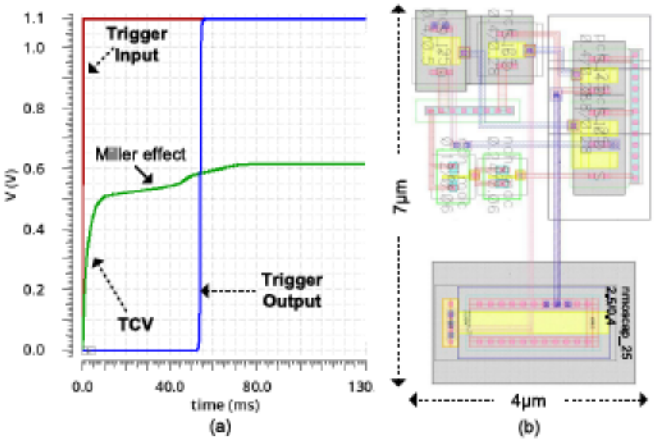

Fig. 9. (a) Simulation result and (b) layout of GL Trojan. The payload signal is generated 60 ms after the input trigger signal.

on gate-oxide tunneling leakage that has a poor correlation with temperature.

E. Performance of Delay-Based Analog Trojans

Analog Trojans are a relatively new form of hardware attack, and only a few examples exist. Table I compares the proposed Trojans with other analog and digital Trojans used for launching various attacks. A2 utilizes the repeated switching in a certain rare scenario to launch an attack. The lower size of A2 is realized through lower capacitance. The trigger output delay of A2 is $5/1$ μs in two versions of the design: one with thick oxide transistor, while another with thin-oxide devices. A2 uses transistors to charge the capacitor and, therefore, is loaded by their leakage current. Compared with this, our implementation is a thick-oxide design and has a trigger output of two days for TC and 60 ms for GL Trojans as they only see GL as the load. A digital privilege escalation attack implementation [38] depends on an extremely rare logic combination but can happen within a few clock cycles.

The 65-nm implementation of thin-oxide implementation of A2 takes approximately 13 μm^2, while the thick-oxide implementation of TC takes 55.5 μm^2. Both A2 and TC Trojans do not require specific inputs for their activation unlike digital Trojans where a logic signal through rare event or combination is needed for activation. Relative to A2, TC does not even need a switching signal, and its activation is solely dependent on the power supply. The power consumption of TC and A2 is comparable, with A2 consuming around 0.5 μW,

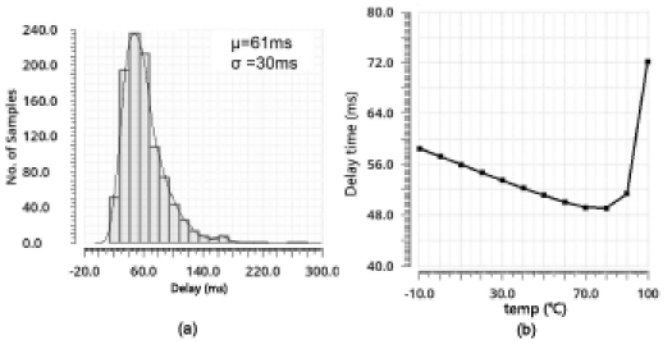

Fig. 10. Simulation of GL Trojan against process and temperature. (a) Process variation of trigger generation. (b) Temperature variation of the trigger.

while TC's peak power consumption around the transition point is 1.5 μW. However, early in the power-up cycle, TC does not show any change in the power level; 1 h after power-up, TC Trojan shows 10-nW power consumption, which is significantly smaller than the level detectable through power side-channel-based Trojan detection methods [7], [39]–[41]. Both TC and GL Trojans can generate large delays with small area overhead, with or without a digital input trigger, and exhibit very low side-channel parameter variation, making them a stealthy fabrication-time hardware attack source.

IV. ANALOG TROJAN ATTACK: AN EXAMPLE CASE STUDY

Analog Trojans are layout Trojans where a malicious foundry will modify the chip layout to insert diodes, capacitors, associated switching circuits, and payload. Sometimes, they can also reuse existing switching transistors and modify an existing gate (e.g., change a buffer to an AND gate) to realize the payload circuit. They can be used to launch variety of attacks, including privilege escalation attack [19], [42], enabling back-door side-channel leakage of critical modules [32], [43], [44], and implementing "kill-switches" [32], [44], among others. To make the attack more stealthy, the analog Trojan can be triggered at run time under the control of software, e.g., intentionally toggling a register bit that is connected to an analog Trojan. They can also have really long trigger time, such as TC Trojan that will be hard to detect through noninvasive testing options.

A. Constructing a Kill-Switch Using TC Trojan

The key feature of analog Trojans is that it can generate a digital logic signal using the analog modalities. An additional

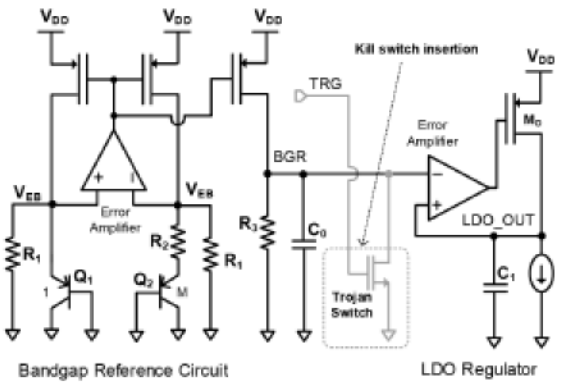

Fig. 11. Constructing a kill-switch by attacking BGR.

digital signal can be used to launch all kinds of attacks on a chip. In this section, we show how a "kill-switch" can be constructed using TC Trojan. We choose the bandgap reference (BGR) circuit as the design vulnerable to Trojan insertion (Trojan Payload). BGR is selected because: 1) it is a relatively large analog circuit with an area in the range of 100 μm $\times$ 100 μm with easily identifiable features due to the large bipolar devices, transistors, and resistors used in the design; 2) it uses capacitors, some of which can be repurposed for Trojan design; and 3) it is the analog reference voltage used for generating on-chip and off-chip power supplies and compromising it and can compromise the whole chip

We used reverse BGR design commonly used in low-voltage, low-power designs [45]. Fig. 11 shows how an attack on BGR can be launched using TC Trojan. The output voltage of BGR, V_{BGR}, is given by

$$V_{\mathrm{BGR}} = \frac{R_3}{R_1}\left(V_{\mathrm{EB}} + \frac{R_1}{R_2}\Delta V_{\mathrm{EB}}\right) \tag{4}$$

where V_{EB} is the base–emitter voltage of the bipolar transistor Q1 and is complementary to absolute temperature (CTAT). ΔV_{EB} is the difference between the base–emitter voltage of Q1 and Q2 and is proportional to absolute temperature (PTAT). The ratioed sum of V_{EB} and ΔV_{EB} produces a reference voltage with very low temperature or process variations. The V_{BGR} voltage is generated through a voltage drop across a resistor. The value of resistors is typically large, from several 100 s of kΩ to MΩ to keep the power low. A large capacitor over 10 s of pF is used at the output to keep the noise level low. Fig. 11 also shows how BGR is used for an LDO.

The payload interface includes an nMOS transistor connected to the output of the BGR. The trigger output generated by TC Trojan stays low keeping the transistor OFF. When the trigger goes high, the bandgap output will be effectively shorted to the ground, which will break the power supply control loop, and the voltage regulation cannot be maintained. The power supply level will drop, and the chip will power down. This operation effectively kills the chip operation.

Fig. 12 shows the layout. Fig. 13 shows the simulation result of the deployment of TC Trojan. Fig. 13(a) shows the power up of the BGR and the LDO regulator. The BGR ramps up to 0.5 V and stabilizes within 10 μs of power up. The LDO output (LDO_OUT) also rises to 0.9 V soon after the BGR powers up. The circuit operation shows that BGR and LDO_OUT

TABLE II
AREA AND POWER BREAKDOWN OF THE TARGET PMU BLOCK

Sub-block and Device	Area	Bias-Current
BJTs Q_1, Q_2	$5625\mu m^2$	$670nA$
R_2 (ΔV_{EB})	$25\mu m^2$	$670nA$
$R_1(V_{EB})$	$1430\mu m^2$	$830nA$
R_3 (BGR)	$112\mu m^2$	$1.8\mu A$
C_0 (BGR)	$91\mu m^2$	-
C_1 (LDO)	$24840\mu m^2$	-
Pass-Device M_O	$70\mu m^2$	-
Error Amplifier-LDO	$42\mu m^2$	$62nA$
Error Amplifier-BGR	$57\mu m^2$	$130nA$
Trojan Switch	$0.2\mu m^2$	$0.8pA$

power up and stabilize. However, the attack from TC Trojan lurks behind without showing any signs. Both LDO and BGR operate without any change in their levels before the Trojan attacks. Once TC Trojan gets deployed, the BGR voltage goes down, and along with it, the LDO also goes down. Fig. 13(b) shows the simulation result of this action. The output of the BGR drops to 0 V once the TC Trojan gets deployed. Since the LDO output is obtained from BGR, it also drops to 50 mV. This will essentially kill the chip and potentially deny service at a critical time. Fig. 12 shows the layout with LDO and BGR (payload circuit) along with the inserted Trojan. Other Trojans can also be inserted without any area overhead, as shown in Fig. 12. The LDO design along with BGR takes an area of 310 μm $\times$ 110 μm. The inserted analog Trojan is 0.16% of the total block area. Table II provides the area and power breakdown of critical blocks of the PMU design.

1) General Application of Analog Trojans: The abovementioned example shows how delay-based analog Trojans can be used to compromise the chip functionality by launching an attack on PMU circuits. An attack on an LDO of a chip through the scan chain has been recently reported in [46] as well. In general, analog circuits present a weak link in securing the chip due to their easily identifiable features. Most analog circuits can be easily identified due to their peculiar layout. BGRs can be identified through their use of bipolar transistors. RF receiver and transmitters can be identified through their use of on-chip inductors. ADCs can be identified through their use of capacitors. The crystal oscillators can be identified through their amplifier design and layout close to I/O pads. The voltage regulators and dc–dc converters are similarly identifiable through their amplifier design and power transistors. Yet, several of these analog circuits are used to provide critical infrastructural functions for the IC. BGR provides the voltage reference for power supplies and ADC. The crystal oscillator is the source of the clock on the chip. RF circuits provide the communication infrastructure. The voltage regulators generate the power supplies for the chip. A highly delayed digital bit from TC or GL Trojans either generated through a power supply or through rare digital input coming from configuration bits (also present in several analog blocks) can be used to simply disable these analog circuits completely, causing the IC to fail immediately.

2) Programmability and Configurability: In this article, we have primarily discussed how the large delay of the proposed Trojan circuits can be used for hardware attacks through a power supply or a digital trigger input. However,

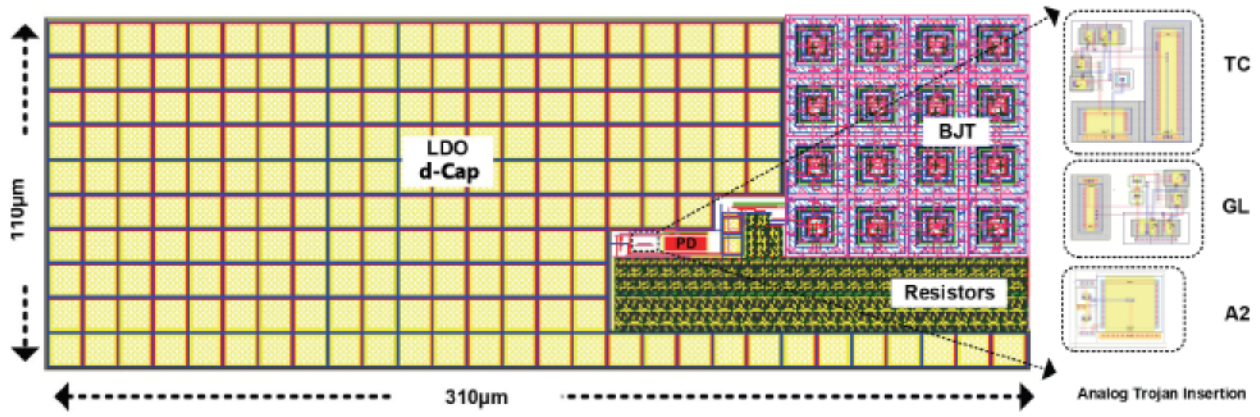

Fig. 12. Layout of LDO and BGR (PMU) with the inserted Trojan kill-switch.

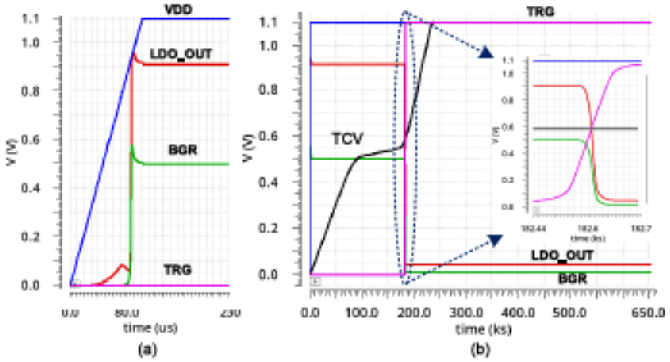

Fig. 13. Simulation result of the BGR and LDO along with the kill-switch activation happening after 170 ks or two days. (a) Power-up of LDO. (b) Deployment of TC Trojan on BGR.

an adversary can also use these Trojans to launch other forms of hardware attacks, while the system is deployed in the field through software programs. In one application scenario, the input trigger of GL and TC Trojans can be connected to one of the configuration bits of a chip. These configuration bits are used to enable sleep-mode, retention mode, or other long-term power management configuration of an IC. These signals will eventually configure the power management and power delivery circuits in a given mode, usually for a long time. As these bits are set for a long time, they can be used to generate a trigger output from the Trojan circuits, which can then be used to change the privilege level by setting or changing a register value, similar to the methods outlined in [19]. The adversary, being aware of the operating mode of the Trojan through the trigger mechanism and its output delay, can utilize the changed privilege to their advantage. This outlines how a privilege can be escalated through TC and GL Trojans. Similarly, the back-door side-channel leakage of critical modules can be enabled as well based on the principles outlined in [32], [43], and [44].

V. Detection Methods

Analog Trojans show significant resilience against conventional prevention and detection methods used against digital Trojans, including exhaustion prevention [47], logic obfuscation [48]–[50], layout camouflaging [51], [52], exhaustive validation [53], and reverse engineering [54].

Prevention techniques, such as activity analysis [55] and exhaustion prevention [47], among others, incorporate periodic steps in the execution flow to prevent charge build-up, which can result in a trigger. However, a more sinister attack, such as "kill-switch," can be incorporated to compromise the global reset of the chip without any stimulus and evade any execution control-based prevention. TC Trojan is based on diode saturation current and may not be caught by periodic resets when the input trigger comes from a power supply. Logic obfuscation [48]–[50] or layout camouflaging [51], [52] has also been proposed for prevention against HTs. They can be effective in protecting a digital IP, but "kill-switch"-based hardware attacks can still be incorporated using analog Trojans. Researchers have also proposed using functional filler cells in the empty space of the IC instead of nonfunctional filler cells, which cannot be validated [56]. The functional filler cells can be verified during chip-validation, and a Trojan using the filler cell can be identified. However, it will add significant validation and area overhead. Also, the adversary can utilize spaces other than filler cells, such as the area used for d-Caps. It is a common design practice to put a decent amount of on-chip d-Caps for signal integrity, and a small change in their value will have little impact on system performance [57]. They are also usually present throughout the chip, including the area around digital IPs. Other Trojan detection methods, such as exhaustive validation [53] and reverse engineering [54], can be employed for detecting the proposed Trojans but may come with additional cost or testing efforts. Side-channel analysis methods analyze the power or temperature map of the chip to detect Trojan's existence but can give a large number of false positives due to significant process variation associated with manufacturing. They also rely on the golden layout of the chip [7], [8].

A. Influence on Side-Channel Parameters

The side-channel analysis is often used for detecting the presence of HT. We analyze the impact of the proposed analog Trojans on side-channel parameters. Since we interface the analog Trojan switch to BGR, a sensitive analog design block, we study its impact on BGR performance. The Trojan insertion includes a min-sized transistor used to short the BGR to the ground. This additional switch can impact the temperature

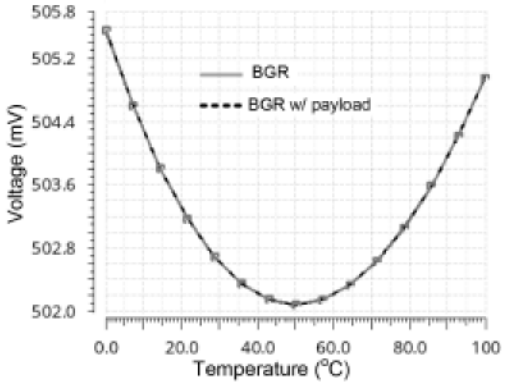

Fig. 14. Variation of BGR voltage with and without Trojan switch insertion.

stability and power consumption of the BGR. Our simulation shows that BGR consumes 2.5 μA, while the Trojan switch consumes 0.8 pA, resulting in an insignificantly small power overhead on BGR. We also simulated the impact of Trojan switch insertion on the BGR output voltage. The designed BGR circuit generates a BGR voltage of 500 mV while realizing temperature stability of 70 ppm/°C. Fig. 14 shows the temperature variation of the BGR circuit. The inserted Trojan switch does not impact the temperature stability of the BGR voltage. Fig. 14 also shows the simulation result when the Trojan switch is inserted. No meaningful difference is noticed between the BGR voltage generated with and without the Trojan switch.

The detection scheme to detect the analog Trojan can also use the change of power consumption due to the insertion of Trojan. Due to the really low value of current used for the realization of the Trojan and an extremely large delay, the proposed Trojans will not show a large variation in power consumption. We simulated the power consumption variation of both TC and GL Trojans and its output across process variation. Fig. 15(a) shows the static power consumption of the PMU block across statistical process variation when a Trojan is not deployed. The mean quiescent current (μ) of 5.20 μA and standard deviation (σ) of 0.26 μA are observed across 1000-point Monte Carlo simulations. We do not see any deviation in the power consumption at $t = 0$ when the Trojan is triggered. For TC Trojan, we also simulated the power consumption variation after 1 h of power up. Fig. 15(b) shows the variation of the quiescent current with a mean (μ) of 5.21 μA and a standard deviation (σ) of 0.26 μA. Even after an hour of being triggered, the TC Trojan does not show distinguishable current variation. Similarly, we simulated the statistical variation of the quiescent current of the PMU after inserting GL Trojan. We observed the quiescent current after 10 ms of the trigger. GL Trojan shows a mean (μ) of 6.12 μA and a standard deviation (σ) of 0.54 μA. GL Trojan-inserted PMU shows an elevated quiescent current but only after several milliseconds of the application of trigger. A detection scheme can be conceived for GL Trojan where power consumption can be observed to identify an elevated value. However, we show the application of Trojan in the PMU unit that drives external loads of hundreds of μA to several hundreds of mA. The elevated power due to analog Trojans becomes insignificant when LDO's output load is considered. Power side-channel-based detection will only have limited success in detecting proposed analog Trojans.

Burn-in Testing: The Burn-in test can be a possible measure for the Trojan detection presented in this article. The TC trojan delay is sensitive to temperature, as shown in Fig. 7(a). However, most burn-in tests for the IC qualification are static and independent of the input test vectors. Given that the TC Trojan can also be configured to be triggered by a digital event, it would be necessary to keep the chip in that given configuration for a longer duration, which will still make detection using burn-in expensive and can be missed even in the dynamic burn-in measurements as the trigger configuration pattern will not be held for a significantly large time. Another interesting point is that with more advanced nodes, burn-in tests could become obsolete as gate dielectric scaling will increase GL exponentially [58], making the proposed Trojans more appealing in the future.

B. Reverse Engineering

Reverse engineering is one of the techniques that can be used to extract the layout details and can also be used to detect the proposed Trojan circuit. The capabilities of reverse engineering a 22-nm chip have been shown in [59]. It involves five processes: namely decapsulation, delayering, imaging, annotation, and schematic creation. With advanced technology node, it continues to be a complex and expensive process and is generally not a part of the regular IC Qualification or production test. Furthermore, dummy transistors and decoupling capacitors are commonly used in analog layout, which can be a potential site for the analog Trojan insertion imparting them stealth from visual inspection during reverse engineering. Also, we present the use case where the Trojan is hidden inside the PMU. However, in a larger design, the Trojan can be made to hide inside a digital block to further provide stealth as is typically done for other HTs. The trigger signal generated by the Trojan is mostly independent of its location in the design.

There are only a few reported works on detection methods for the newly emerging analog Trojans [22], [23], both relying on a toggling input for the Trojan. The technique proposed in [23] is a run-time detection method, which counts the toggling rate of a suspicious register bit and stops it once it reaches a preset threshold. The premise of this approach is to disable the charging of the C_t capacitor [see Fig. 1(a)] through switching to prevent it to reach the required threshold needed for trigger output. However, this method may have a high false-positive rate and can disrupt regular program execution if a certain register is indeed toggling frequently. Another recently proposed detection method based on information flow tracking (IFT) [22] is at the validation time. It again assumes a toggling input for the analog Trojan, and the Trojan also characterizes a large capacitor. However, not all analog Trojans require large capacitors and toggling input as our own analysis shows. This method is also invasive, requiring expensive chip deprocessing to obtain the design layout for identifying large capacitors. TC and GL Trojans will also evade detection techniques that employ reducing Trojan's activation time [60], as their timing is generated through passive leakage.

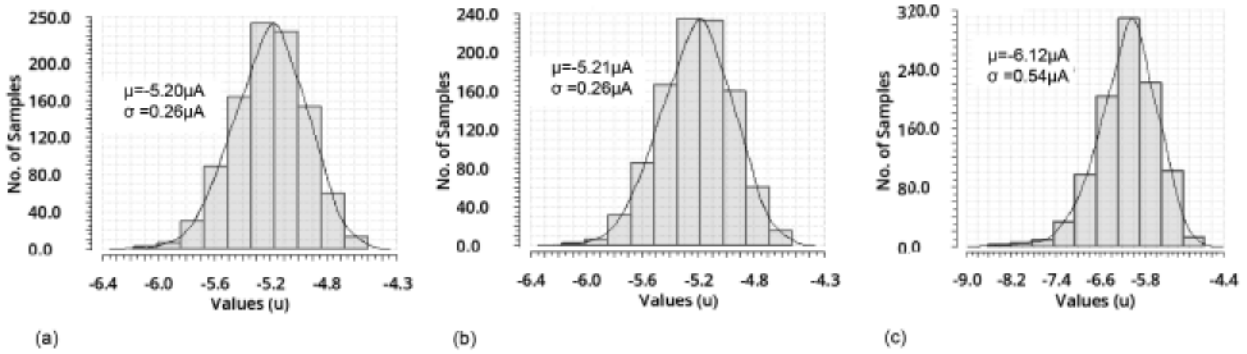

Fig. 15. Simulation result of the variation of BGR and LDO quiescent current with and without analog Trojans for side-channel detection. (a) Statistical variation of the PMU quiescent current without analog Trojan. (b) Variation of the quiescent current with TC Trojan after 1 h of the trigger. (c) Variation of the quiescent current with GL Trojan after 10 ms of the trigger.

VI. Conclusion

In this article, we proposed large delay-based analog Trojan circuits that can be interfaced with digital and analog macros to launch fabrication-time hardware attacks. Large delay is generated using a combination of gate-oxide leakage current or diode's reverse saturation current and the Miller capacitance-based circuits. The proposed circuits can generate trigger signals to payload after two days and 60 ms after the application of the trigger. Such large delays and the ability to operate across multiple power domains will make the detection of these analog Trojans very challenging. In addition, the proposed designs have a small area footprint and show very limited side-channel power leakage for detection. We also investigated the impact of process and temperature variation of the design and possible detection methods for detecting proposed Trojans. Thick-oxide leakage modeling was implemented to study the robustness of the proposed design. We showed the usage of proposed Trojans to launch an attack on the PMU unit of an IC to construct a kill-switch. The simulation results show that this kind of attack is covert and effective.

References

[1] A. Chatterjee, D. Gudmundsson, R. K. Nurani, S. Seshadri, and J. G. Shanthikumar, "Fabless-foundry partnership: Models and analysis of coordination issues," *IEEE Trans. Semicond. Manuf.*, vol. 12, no. 1, pp. 44–52, Feb. 1999.

[2] Y. Liu, Y. Jin, A. Nosratinia, and Y. Makris, "Silicon demonstration of hardware trojan design and detection in wireless cryptographic ICs," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 25, no. 4, pp. 1506–1519, Apr. 2017.

[3] A. Sengupta and S. Kundu, "Guest editorial securing IoT hardware: Threat models and reliable, low-power design solutions," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 25, no. 12, pp. 3265–3267, Dec. 2017.

[4] G. T. Becker, F. Regazzoni, C. Paar, and W. P. Burleson, "Stealthy dopant-level hardware trojans," in *Cryptographic Hardware and Embedded Systems—CHES*, G. Bertoni and J.-S. Coron, Eds. Berlin, Germany: Springer, 2013, pp. 197–214.

[5] R. Kumar, P. Jovanovic, W. Burleson, and I. Polian, "Parametric trojans for fault-injection attacks on cryptographic hardware," in *Proc. Workshop Fault Diagnosis Tolerance Cryptogr.*, Sep. 2014, pp. 18–28.

[6] T. Sugawara *et al.*, "Reversing stealthy dopant-level circuits," *J. Cryptograph. Eng.*, vol. 5, no. 2, pp. 85–94, Jun. 2015, doi: 10.1007/s13389-015-0102-5.

[7] D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi, and B. Sunar, "Trojan detection using IC fingerprinting," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2007, pp. 296–310.

[8] Y. Jin and Y. Makris, "Hardware trojan detection using path delay fingerprint," in *Proc. IEEE Int. Workshop Hardw.-Oriented Secur. Trust*, Jun. 2008, pp. 51–57.

[9] M. Potkonjak, A. Nahapetian, M. Nelson, and T. Massey, "Hardware trojan horse detection using gate-level characterization," in *Proc. 46th Annu. Design Autom. Conf. ZZZ - DAC*, Jul. 2009, pp. 688–693.

[10] S. Narasimhan, X. Wang, D. Du, R. S. Chakraborty, and S. Bhunia, "TeSR: A robust temporal self-referencing approach for hardware trojan detection," in *Proc. IEEE Int. Symp. Hardw.-Oriented Secur. Trust*, Jun. 2011, pp. 71–74.

[11] S. Adee, "The hunt for the kill switch," *IEEE Spectr.*, vol. 45, no. 5, pp. 34–39, May 2008.

[12] Y. Alkabani and F. Koushanfar, "Extended abstract: Designer's hardware trojan horse," in *Proc. IEEE Int. Workshop Hardw.-Oriented Secur. Trust*, Jun. 2008, pp. 82–83.

[13] S. T. King, J. Tucek, A. Cozzie, C. Grier, W. Jiang, and Y. Zhou, "Designing and implementing malicious hardware," in *Proc. 1st Usenix Workshop Large-Scale Exploits Emergent Threats*, 2008, pp. 1–8.

[14] Y. Shiyanovskii, F. Wolff, A. Rajendran, C. Papachristou, D. Weyer, and W. Clay, "Process reliability based trojans through NBTI and HCI effects," in *Proc. NASA/ESA Conf. Adapt. Hardw. Syst.*, Jun. 2010, pp. 215–222.

[15] C. Dunbar and G. Qu, "Designing trusted embedded systems from finite state machines," *ACM Trans. Embedded Comput. Syst.*, vol. 13, no. 5s, pp. 1–20, Dec. 2014, doi: 10.1145/2638555.

[16] H. Liu, H. Luo, and L. Wang, "Design of hardware trojan horse based on counter," in *Proc. Int. Conf. Qual., Rel., Risk, Maintenance, Saf. Eng.*, Jun. 2011, pp. 1007–1009.

[17] A. Iyengar and S. Ghosh, *Hardware Trojans and Piracy of PCBs*. Cham, Switzerland: Springer, 2018, pp. 125–145.

[18] S. Ghandali, T. Moos, A. Moradi, and C. Paar, "Side-channel hardware trojan for provably-secure SCA-protected implementations," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 28, no. 6, pp. 1435–1448, Jun. 2020.

[19] K. Yang, M. Hicks, Q. Dong, T. Austin, and D. Sylvester, "a2: Analog malicious hardware," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2016, pp. 18–37.

[20] Y. Kim *et al.*, "Flipping bits in memory without accessing them: An experimental study of DRAM disturbance errors," in *Proc. ACM/IEEE 41st Int. Symp. Comput. Archit. (ISCA)*, Jun. 2014, pp. 361–372. [Online]. Available: http://dl.acm.org/citation.cfm?id=2665671.2665726

[21] Z. B. Aweke *et al.*, "ANVIL: Software-based protection against next-generation rowhammer attacks," in *Proc. Twenty-First Int. Conf. Architectural Support Program. Lang. Operating Syst. ASPLOS*, 2016, pp. 743–755, doi: 10.1145/2872362.2872390.

[22] X. Guo, H. Zhu, Y. Jin, and X. Zhang, "When capacitors attack: Formal method driven design and detection of charge-domain trojans," in *Proc. Design, Autom. Test Eur. Conf. Exhib. (DATE)*, Mar. 2019, pp. 1727–1732.

[23] Y. Hou, H. He, K. Shamsi, Y. Jin, D. Wu, and H. Wu, "R2D2: Runtime reassurance and detection of a2 trojan," in *Proc. IEEE Int. Symp. Hardw. Oriented Secur. Trust (HOST)*, Apr. 2018, pp. 195–200.

[24] J. H. Saltzer and M. F. Kaashoek, *Principles of Computer System Design*. San Mateo, CA, USA: Morgan Kaufmann, 2009, ch. 8, p. 58.

[25] M. Seaborn. *Exploiting the DRAM Rowhammer Bug to Gain Kernel Privileges*. Accessed: Mar. 22, 2020. [Online]. Available: https://googleprojectzero.blogspot.com/2015/03/exploiting-dram-rowhamme%r-bug-to-gain.html

[26] S. Hong, P. Frigo, Y. Kaya, C. Giuffrida, and T. Dumitras, "Terminal brain damage: Exposing the graceless degradation in deep neural networks under hardware fault attacks," in *Proc. 28th USENIX Secur. Symp. (USENIX Secur.)*, Santa Clara, CA, USA: USENIX Association, Aug. 2019, pp. 497–514. [Online]. Available: https://www.usenix.org/conference/usenixsecurity19/presentation/hong

[27] A. Tatar, R. K. Konoth, E. Athanasopoulos, C. Giuffrida, H. Bos, and K. Razavi, "Throwhammer: Rowhammer attacks over the network and defenses," in *Proc. USENIX Conf. Usenix Annu. Tech. Conf.*, 2018, pp. 213–225.

[28] A. Kwong, D. Genkin, D. Gruss, and Y. Yarom, "RAMBleed: Reading bits in memory without accessing them," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2020, pp. 1–17.

[29] M. N. I. Khan, A. De, and S. Ghosh, "Cache-out: Leaking cache memory using hardware trojan," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 28, no. 6, pp. 1461–1470, Jun. 2020.

[30] A. De, M. Nasim Imtiaz Khan, K. Nagarajan, and S. Ghosh, "HarTBleed: Using hardware trojans for data leakage exploits," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 28, no. 4, pp. 968–979, Apr. 2020.

[31] Q. Wang, D. Chen, and R. L. Geiger, "Transparent side channel trigger mechanism on analog circuits with PAAST hardware trojans," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, May 2018, pp. 1–4.

[32] K. Xiao, D. Forte, Y. Jin, R. Karri, S. Bhunia, and M. Tehranipoor, "Hardware trojans: Lessons learned after one decade of research," *ACM Trans. Design Autom. Electron. Syst.*, vol. 22, no. 1, pp. 1–23, Dec. 2016, doi: 10.1145/2906147.

[33] R. C. Neville, "Solar cell configuration and performance," in *Solar Energy Conversion*, 2nd ed, R. C. Neville, Ed. Amsterdam, The Netherlands: Elsevier, 1995, pp. 197–256. [Online]. Available: http://www.sciencedirect.com/science/article/pii/B9780444898180500065

[34] G. Timp *et al.*, "The relentless march of the MOSFET gate oxide thickness to zero," *Microelectron. Rel.*, vol. 40, nos. 4–5, pp. 557–562, Apr. 2000. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0026271499002577

[35] ITRS Test Working Group, "International Technology Roadmap for Semiconductors (ITRS) 2.0: Test and test equipment," ITRS, London, U.K., Tech. Rep., 2015. [Online]. Available: https://www.semiconductors.org/wp-content/uploads/2018/06/0_2015-ITRS%2.0-Test-.pdf

[36] R. Dixit. (Feb. 2017). *Adrressing Test-Time Challenges*. [Online]. Available: https://semiengineering.com/addressing-test-time-challenges/

[37] N. Paydavosi *et al.*, "BSIM4v4.8.0 MOSFET model user's manual," EECS Dept., Univ. California, Berkeley, Berkeley, CA, USA, Tech. Rep., 2013.

[38] M. Hicks, M. Finnicum, S. T. King, M. M. K. Martin, and J. M. Smith, "Overcoming an untrusted computing base: Detecting and removing malicious hardware automatically," in *Proc. IEEE Symp. Secur. Privacy*, May 2010, pp. 159–172.

[39] S. Narasimhan *et al.*, "Hardware trojan detection by multiple-parameter side-channel analysis," *IEEE Trans. Comput.*, vol. 62, no. 11, pp. 2183–2195, Nov. 2013.

[40] Y. Tang, S. Li, L. Fang, X. Hu, and J. Chen, "Golden-chip-free hardware trojan detection through quiescent thermal maps," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 27, no. 12, pp. 2872–2883, Dec. 2019.

[41] R. Rad, J. Plusquellic, and M. Tehranipoor, "A sensitivity analysis of power signal methods for detecting hardware trojans under real process and environmental conditions," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 18, no. 12, pp. 1735–1744, Oct. 2010.

[42] N. G. Tsoutsos and M. Maniatakos, "Fabrication attacks: Zero-overhead malicious modifications enabling modern microprocessor privilege escalation," *IEEE Trans. Emerg. Topics Comput.*, vol. 2, no. 1, pp. 81–93, Mar. 2014.

[43] L. Lin, W. Burleson, and C. Paar, "MOLES: Malicious off-chip leakage enabled by side-channels," in *Proc. Int. Conf. Comput.-Aided Design – ICCAD*, Nov. 2009, pp. 117–122.

[44] S. Kelly, X. Zhang, M. Tehranipoor, and A. Ferraiuolo, "Detecting hardware trojans using on-chip sensors in an ASIC design," *J. Electron. Test.*, vol. 31, no. 1, pp. 11–26, Feb. 2015, doi: 10.1007/s10836-015-5504-x.

[45] H. Banba *et al.*, "A CMOS bandgap reference circuit with sub-1-V operation," *IEEE J. Solid-State Circuits*, vol. 34, no. 5, pp. 670–674, May 1999.

[46] M. Elshamy, G. Di Natale, A. Pavlidis, M.-M. Louerat, and H.-G. Stratigopoulos, "Hardware trojan attacks in analog/mixed-signal ICs via the test access mechanism," in *Proc. IEEE Eur. Test Symp. (ETS)*, May 2020, pp. 1–6.

[47] V. van der Veen *et al.*, "Drammer: Deterministic rowhammer attacks on mobile platforms," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2016, pp. 1675–1689, doi: 10.1145/2976749.2978406.

[48] R. S. Chakraborty and S. Bhunia, "Security against hardware trojan through a novel application of design obfuscation," in *Proc. Int. Conf. Comput.-Aided Design – ICCAD*, Nov. 2009, pp. 113–116, doi: 10.1145/1687399.1687424.

[49] J. A. Roy, F. Koushanfar, and I. L. Markov, "Ending piracy of integrated circuits," *Computer*, vol. 43, no. 10, pp. 30–38, Oct. 2010.

[50] T. E. Schulze, D. G. Beetner, Y. Shi, K. A. Kwiat, and C. A. Kamhoua, "Combating data leakage trojans in commercial and ASIC applications with time-division multiplexing and random encoding," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 26, no. 10, pp. 2007–2015, Oct. 2018.

[51] R. P. Cocchi, J. P. Baukus, L. W. Chow, and B. J. Wang, "Circuit camouflage integration for hardware IP protection," in *Proc. The 51st Annu. Design Autom. Conf. Design Autom. Conf. – DAC*, Jun. 2014, pp. 1–5.

[52] J. Rajendran, M. Sam, O. Sinanoglu, and R. Karri, "Security analysis of integrated circuit camouflaging," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur. – CCS*, 2013, pp. 709–720, doi: 10.1145/2508859.2516656.

[53] S. Bhunia, M. S. Hsiao, M. Banga, and S. Narasimhan, "Hardware trojan attacks: Threat analysis and countermeasures," *Proc. IEEE*, vol. 102, no. 8, pp. 1229–1247, Aug. 2014.

[54] C. Bao, D. Forte, and A. Srivastava, "On application of one-class SVM to reverse engineering-based hardware trojan detection," in *Proc. 15th Int. Symp. Qual. Electron. Design*, Mar. 2014, pp. 47–54.

[55] G. I. Apecechea, T. Eisenbarth, and B. Sunar, "MASCAT: Stopping microarchitectural attacks before execution," *IACR Cryptol. ePrint Arch.*, vol. 2016, p. 1196, 2016. [Online]. Available: https://eprint.iacr.org/

[56] K. Xiao and M. Tehranipoor, "BISA: Built-in self-authentication for preventing hardware trojan insertion," in *Proc. IEEE Int. Symp. Hardw.-Oriented Secur. Trust (HOST)*, Jun. 2013, pp. 45–50.

[57] M. D. Pant, P. Pant, and D. S. Wills, "On-chip decoupling capacitor optimization using architectural level prediction," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 10, no. 3, pp. 319–326, Jun. 2002.

[58] S. Borkar, "Tackling variability and reliability challenges," *IEEE Design Test Comput.*, vol. 23, no. 6, p. 520, Nov. 2006.

[59] Chipworks. (Apr. 2012). *Intel's 22-nm Tri-gate Transistors Exposed*. [Online]. Available: http://www.chipworks.com/en/technical-competitive-analysis/resources/blog/intels-22-nm-tri-gate-transistors-exposed/

[60] H. Salmani, M. Tehranipoor, and J. Plusquellic, "A novel technique for improving hardware trojan detection and reducing trojan activation time," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 20, no. 1, pp. 112–125, Jan. 2012.