Digital-to-Analog Hardware Trojan Attacks

Mohamed Elshamy, Giorgio Di Natale, Alhassan Sayed, Antonios Pavlidis, Marie-Minerve Louërat, Hassan Aboushady, Haralampos-G. Stratigopoulos

Digital-to-Analog Hardware Trojan Attacks

Mohamed Elshamy, Giorgio Di Natale, *Senior Member, IEEE*, Alhassan Sayed, Antonios Pavlidis, Marie-Minerve Louërat, Hassan Aboushady, *Senior Member, IEEE*, and Haralampos-G. Stratigopoulos, *Member, IEEE*

***Abstract*—We propose a Hardware Trojan (HT) attack for analog circuits with its key characteristic being that it cannot be prevented or detected in the analog domain. The HT attack works in the context of Systems-on-Chip (SoCs) comprising both digital and analog Intellectual Property (IP) blocks. The attacker could be either the SoC integrator or the foundry. More specifically, the HT trigger is placed inside a dense digital IP block where it can be effectively hidden, whereas the HT payload is in the form of a digital pattern transported via the test bus or generated within the test bus, reaching the Design-for-Test (DfT) or programmability interface of the victim analog IP with the test bus. The HT payload unexpectedly activates the DfT and sets the victim analog IP into some possibly partial and undocumented test mode or changes the nominal programmability. The HT payload can be designed to result in performance degradation or complete malfunction, i.e., denial of service. We demonstrate this HT attack scenario on two analog IPs, namely a low-dropout (LDO) regulator using simulation and an RF receiver using hardware measurements.**

***Index Terms*—Hardware security and trust, hardware Trojans, test access and control mechanisms, analog and mixed-signal integrated circuits.**

I. Introduction

The globalization of the Integrated Circuit (IC) design and fabrication steps has introduced an horizontal IC design model where the design of a single chip involves many different parties, i.e., Computer-Aided Design (CAD) tool providers, Intellectual Property (IP) block providers, System-on-Chip (SoC) integrators, foundries, etc. As a result, the IC design travels through many parties which introduces many points where an attack may be staged. Attack scenarios include cloning, counterfeiting, IC overbuilding, reverse engineering, and Hardware Trojan (HT) insertion. This work deals with HT attacks which are a major preoccupation for society, industry, governments, and military, since they pose severe risks with possibly disastrous outcomes. For this reason, HTs have received major attention in the scientific community throughout the last two decades [1], [2].

Manuscript received April 12, 2021; revised July 24, 2021, and August 30, 2021; accepted September 16, 2021. This work was supported by the ANR STEALTH project under Grant ANR-17-CE24-0022-01 and by the RAPID FLEXyRADIO project. This article was recommended by Associate Editor P. Rombouts. (Corresponding author: Haralampos-G. Stratigopoulos.)

Mohamed Elshamy, Antonios Pavlidis, Marie-Minerve Louërat, Hassan Aboushady, and Haralampos-G. Stratigopoulos are with the Sorbonne Université, CNRS, LIP6, 75005 Paris, France (e-mail: mohamed.elshamy@lip6.fr; antonios.pavlidis@lip6.fr; marie-minerve.louerat@lip6.fr hassan.aboushady@lip6.fr; haralampos.stratigopoulos@lip6.fr).

Giorgio Di Natale is with the Université Grenoble Alpes, CNRS, TIMA, 38000 Grenoble, France (e-mail: giorgio.di-natale@univ-grenoble-alpes.fr).

Alhassan Sayed is with the Sorbonne Université, CNRS, LIP6, 75005 Paris, France, and also with the Electronics and Communications Department, Minia University, Minia 61519, Egypt (e-mail: alhassan.sayed@lip6.fr).

Digital Object Identifier 10.1109/TCSI.2021.XXXXXXX

A HT is a malicious modification of the design performed by an attacker within the IC supply chain that is intent to stay hidden and evade detection by the end-user who is the defender in this case. The HT is an undocumented functionality for the end-user and is designed in such a way that once activated it is capable of performing an undesired effect for the end-user. The motivation for inserting a HT includes leaking sensitive information out of the chip, e.g., cipher keys, degrading the performance of the chip, or leading to complete malfunction, e.g., denial-of-service.

Any HT is in general composed of a trigger and a payload mechanism. The HT may be always-on, in which case strictly speaking there is no trigger mechanism, it may be uncontrollably activated based on some rare conditions occurring, or it may have a well-timed activation controlled by the attacker leaving a time bomb into the design. The payload mechanism refers to the HT effect on the chip's functionality.

In addition to the HT activation mechanism and HT effect, a commonly used taxonomy of HTs considers the insertion phase, the abstraction level, and the HT location on the die. A HT may be inserted by the CAD tool provider, i.e., by compromising the synthesis or verification scripts, by an IP design team, by a SoC integrator that can manipulate both the third-party IP (3PIP) cores and the test infrastructure comprising the test access and control mechanism and several embedded test instruments, and by a foundry that receives the GDSII file. A HT may be inserted at system-level, register-transfer level (RTL), gate-level, or layout-level. The location of the HT could be anywhere on the die, i.e., digital processor, memory, power management unit, analog cores, etc.

There is a multitude of HT designs proposed in the literature that range from simple to very complex attack modes. The simplest HTs are combinational circuits that monitor a set of nodes to generate a trigger on the simultaneous occurrence of rare node conditions and, subsequently, once the trigger is activated, the payload is simply flipping the value of another node. Another category of simple HTs are the sequential HTs which also have a condition-based activation, but they are triggered with a sequence of conditions and not with a specific state or condition like the combinational HTs. More complex HTs include silicon wearout mechanisms [3], hidden side-channels [4], changing dopant polarity in active areas of transistors [5], siphoning charge from victim wires [6], etc.

From the attacker's perspective, the goal is to achieve the desired effect via the use of a stealthy and minimum footprint HT such that it evades pre-silicon prevention and post-silicon detection methods applied by the defender.

Pre-silicon prevention methods include: (a) functional verification of 3PIP cores [7]; (b) structural analysis of Hardware Description Language (HDL) codes [7]; (c) targeted automatic

test pattern generation algorithms [8] or simulating the circuit using specific test benches, i.e., performing aging simulations along with over-clocking [9] or short-term aging [10] to magnify the effect of the HT without triggering it; (d) searching for unused components during design-time verification and removing them as potentially suspicious [11]; (e) filling in all unused spaces on the layout, which are most likely insertion areas for HTs, with functional filler cells and checking if those have changed [12]; and (f) design obfuscation, for example using locking [13], [14], camouflaging [15], [16], or split manufacturing [17], aiming at obscuring the IC functionality so as to make it difficult for the attacker to insert the HT.

Post-silicon detection methods include: (a) destructive reverse-engineering, which involves de-packaging and de-layering the chip, imaging the chip's layers, and using software to stitch together the prepared images, thereby recovering the layout and netlist, which thereafter can be carefully examined to detect the presence of HTs [18], [19]; (b) optical circuit analysis aiming at measuring optical emissions of the IC and comparing them with a trusted emission image of a "golden" IC [20]; (c) functional testing aiming at exposing the HT by applying test patterns [8]; (d) statistical side-channel fingerprinting aiming at exposing the HT by its effect on parametric measurements, i.e., delay, power, temperature, etc. [21], [22]; and (e) using run-time monitors, i.e., current sensors [23] and thermal sensors [24].

To date, the vast majority of HT attacks and defenses have been demonstrated for digital ICs [25]. Few HT designs have been demonstrated in the analog domain, including HTs inserted into the RF front-end aiming at leaking sensitive information via a covert side-channel [26]–[29] and HTs that bring the analog IC into an undesired state or operation mode [30]–[34]. The prior art on HT in the analog domain will be reviewed in more detail in Section II.

In general, designing HTs for analog ICs is very challenging since all criteria that make up an effective HT are difficult to meet. First, it is difficult to design stealthy HT since analog signal paths are typically very sensitive and a HT circuitry tapping into them is likely to result in some non-negligible performance degradation, thus it will be difficult for the infected IC to pass testing. Second, it is difficult to design small footprint HTs that will evade optical reverse engineering since analog designs comprise few components or can be clearly divided into sub-blocks or stages each comprising few components. Third, on any analog IC we can extract several information-rich measurements, such that it is unlikely not to be able to find a measurement subspace wherein the statistical fingerprints of HT-infected and HT-free instances are clearly distinguished.

In this paper, we propose a HT attack for analog ICs with its key characteristic being that it is invisible in the analog domain [35]. This is achieved by exploiting the on-chip test infrastructure that is common to digital and analog cores within the SoC. In particular, the HT trigger mechanism resides in a digital IP core and the payload mechanism resides in the test bus that links all IP blocks in the SoC in a daisy network. The HT is triggered in the dense digital section of the SoC, thus posing challenge for HT prevention or detection. The HT payload is transferred to the victim analog IP via the test bus and the interface of the analog IP to the test bus. The interface can include Design-for-Test (DfT) blocks, i.e., sensors and actuators, and programmability fabric for the purpose of calibration. The proposed HT is demonstrated on two case studies. The first case study shown with simulation is a low-dropout (LDO) regulator where the HT infects it via its DfT interface. The second case study shown with hardware measurements is an RF receiver front-end where the HT infects it via its programmability fabric.

The rest of the paper is structured as follows. In Section II, we review the prior art on HT attacks in the analog domain. In Section III, we provide an overview of DfT techniques for Analog and Mixed-Signal (A/M-S) and RF ICs. In Section IV, we provide an overview of calibration schemes present in A/M-S and RF ICs. In Section V, we review a modern test infrastructure and its use for accessing and controlling DfT structures and the programmability fabric. In Section VI, we present the proposed HT attack scenarios. In Sections VII and VIII, we demonstrate the HT attack on the two case studies. Section IX concludes the paper.

II. Prior art on HT attacks in the analog domain

In [26]–[29], HT attacks are demonstrated for wireless ICs aiming at leaking secret information within a legitimate signal transmission. The attacker leverages the data transmission capability of the HT-infected device to establish a covert side-channel, without the need to gain physical access to the device. For example, the HT could forward bit-by-bit the content of the cipher key register of the crypto-core to the analog transmitter. In [26], [27], [29], the idea is to exploit the margins that exist between the operating point of the transmitter and the boundaries defined by the transmitter and communication standard specifications. In particular, the HT performs minute modifications in the parameters of the transmitted signal, such as amplitude and frequency, to leak sensitive information from the tampered device. Two HT payload mechanisms are shown in [29], one that uses a single pole double throw switch and a pair of resistors to alter the input termination impedance of the power amplifier, and another one that reprograms the gain stages. In [28], it is proposed to use spread spectrum techniques to hide an unauthorized transmission signal within the legitimate signal below the noise level. For all the aforementioned HT attacks, the IC passes all conventional specification tests and the transmission signal still obeys the transmission specifications and is within the margins allowed because of process variations. Therefore, the inconspicuous receiver cannot interpret the minute change in the transmitted signal as malicious. However, the attacker knowing the HT payload mechanism can listen to the channel and recover the key. It has been demonstrated that this type of HTs can be detected by statistical side-channel fingerprinting [27], careful analysis of the transmitted signal spectrum [28], or adaptive channel estimation [29], which leverages the slow-fading characteristics of indoor communication channels to distinguish between channel impairments and HT activity.

Another interesting direction for HT design is to exploit the fact that an analog IC may have undesired states or

operation modes. In this case, the HT attack consists of bringing the analog IC into one of these states to cause undesirable operation. This HT type has been demonstrated for a multitude of basic analog circuits, such as current mirrors, filters, oscillators, bandgap reference sources and operational amplifiers [30]–[34].

III. DfT for A/M-S and RF ICs

DfT consists in embedding test structures on-chip with the aim to improve defect coverage and/or facilitate testing, i.e., reduce the test cost by speeding up test application time and/or alleviating the dependence on complex Automatic Test Equipment (ATE). Built-in Self-test (BIST) is a special form of DfT where the test procedure takes place entirely on-chip without needing to interface the chip to external ATE. In post-manufacturing testing, BIST can offer significant test cost savings at the expense of larger area overhead. For safety-critical or mission-critical applications, it can be reused in the field of operation to perform on-line test in idle times or concurrent error detection.

In general, for A/M-S and RF ICs, the DfT circuitry can comprise one or more of the following test structures: test access points, digitally-controlled re-configuration schemes, and test instruments, i.e., test stimulus generators, actuators, sensors, checkers, and test response analyzers.

Examples of generic DfT techniques include oscillation-based testing [36], topology modification [37], and symmetry-based BIST [38]. In oscillation-based testing, the circuit is re-configured in a positive feedback loop to force oscillation. Then, the oscillation frequency and amplitude are measured on-chip using as test response analyzer a counter and amplitude detector, respectively. Deviations from the nominal expected oscillation frequency and amplitude point to defect detection. In topology modification, 1-bit controlled Pull-Down (PD) and Pull-Up (PU) transistors are used to tie a node to V_{dd} or ground, respectively, with the aim of re-configuring the circuit such that defects are better exposed. In symmetry-based BIST, invariant properties, i.e., properties that hold true in error-free operation but are violated in the presence of defects, are built and monitored by checkers.

There exist also DfT techniques that are specific to the circuit class, i.e., linear time-invariant circuits, Phase-Locked Loops (PLLs), data converters, RF transceivers, etc., and oftentimes specific to different architectures within a circuit class.

For linear time-invariant circuits, concurrent error detection is achieved by checkers that monitor checksums [39] or create a pseudo-duplicated response that by default in error-free operation converges to the circuit output [40].

For Analog-to-Digital Converters (ADCs), traditional BIST schemes for static linearity testing, i.e., Differential Non-Linearity (DNL) and Integral Non-Linearity (INL), use test stimulus generation performed by ramp generators [41] and a test response analyzer that computes the histogram [42], which could be done also based on reduced-code collection [43]. The requirement for a high-resolution test stimulus can be relaxed by using non-linear stimulus generators combined with advanced post-processing techniques of the converter's output [44]. Traditional BIST schemes for dynamic testing, i.e., Signal-to-Noise Ratio (SNR), use test stimulus generation performed by sinusoidal signal generators [45], [46] or $\Sigma\Delta$ bitsteams encoding sinusoidal signals [47], and test response analyzers that perform spectral analysis [48] or sine-wave fitting analysis [47].

For PLLs, BIST techniques have been proposed for measuring on-chip the jitter [49], [50]. The PLL response is under-sampled and the count of unstable bits at the clock rising edges is correlated to the high-frequency jitter. Defect-oriented BIST for PLLs has been proposed in [51], where a digital Pseudo-Random Bit Sequence (PRBS) injected in the charge pump perturbs the PLL, and the cross-correlation of the PRBS pattern with the output of the phase/frequency detector is considered for defect detection.

For RF transceivers, a common BIST technique consists in creating a loop-back connection between the transmitter and the receiver, in order to test the whole RF transceiver, e.g., measure the Error Vector Magnitude (EVM), using baseband only signals [52], [53].

Sensor-based testing is another common DfT technique. Current sensors [54] and amplitude detectors [55] can be used to monitor current or voltage on internal nodes. There exist also non-intrusive sensors that extract information without being electrically connected to the circuit under test, e.g., temperature sensors [56] and process variation-aware sensors [57].

IV. Calibration of A/M-S and RF ICs

Calibration schemes are oftentimes utilized in A/M-S and RF ICs with the aim of boosting yield, i.e., by compensating against process variations and non-idealities, and to program different operation modes, e.g., in the case of multi-standard RF transceivers [58], [59]. Embedding calibration in A/M-S and RF ICs becomes essential especially in advance technology nodes since such designs suffer from yield loss due to model immaturity and variability caused by parasitics and layout-dependent effects.

At a minimum, a calibration scheme utilizes digitally-controlled tuning knobs that act on the circuit performances. Tuning knobs may include bias voltages, current sources, or single tunable components, such as resistors, capacitors, and varactors.

The standard calibration algorithm consists in multiple testing/tuning iterations where in each step the performances are measured and the next best tuning knob setting is dictated based on some optimization algorithm.

The calibration scheme may also utilize on-chip sensors for performance measurement which can speed-up the test cycle and alleviate the dependence on complex ATE. For example, one-shot calibration schemes based on process-variation-aware sensors and machine learning are proposed in [60], [61].

The most advance calibration schemes are fully implemented on-chip rendering the circuit self-healing. These schemes can also be used during the lifetime of the circuit to compensate against aging. They comprise tuning knobs or actuators, sensors for extracting information-rich measurements

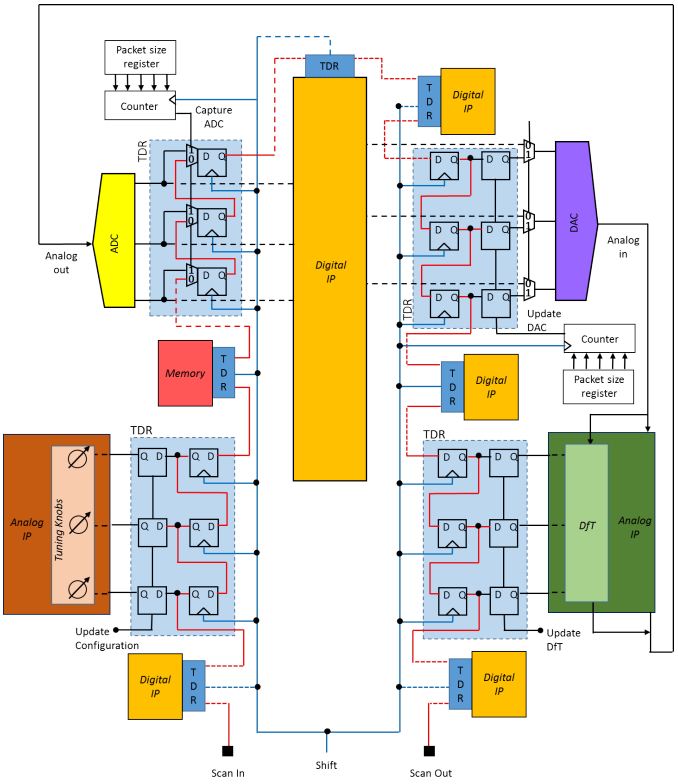


Fig. 1: Scan access including analog IPs (adapted from [64]).

or directly the performances, and a digital processor engine that maps the outputs of the sensors to tuning knob values and aims at driving the optimization so as to identify a good balance among multiple competing performance goals [62], [63].

V. Test Access and Control Mechanism in SoCs

A modern SoC can embed numerous IP blocks and, in turn, each IP block typically embeds a variety of DfT structures, i.e., test access points and test instruments, and comes with a calibration scheme that uses a programmability interface. The total number of DfT structures and tuning knobs in a SoC can easily be in the order of hundreds or even thousands, and accessing them separately from primary pins is prohibitive.

To this end, an on-chip test infrastructure is used that connects all the DfT structures and programming interfaces to a common test bus, in order to gain access and control them, manage the test and calibration process, and offload the test response to the ATE for off-chip test response analysis, all-in-all using a limited number of dedicated primary pins [65]. The test bus is interfaced on the chip boundary with the test access port (TAP). Typically, each IP block has its own test program, i.e., IP-level test patterns, and once the SoC design is finalized and the test infrastructure is added, the test programs are re-targeted to the top-level design. The test programs can be simply concatenated, but to achieve higher test time efficiency they can be regrouped enabling concurrency.

The test infrastructure is standardized driven by the needs for test portability and re-use [65]. Portability refers to reusing a test program independently of the position of the target IP block inside the SoC hierarchy, reusing a test program at different steps, i.e., post-manufacturing test, debugging, in-field test towards dependable designs, etc., and reusing a test program independently of the ATE platform. Standardization dissociates the IP block-level DfT structure and programming interface design from test application and calibration operations at SoC-level, i.e., access, control, observe, program, etc., and allows all actors, i.e., IP providers, SoC integrators, test infrastructure providers, to speak the same language. It also enables test automation using CAD tools and leads to significant SoC-level test time reduction.

The latest standard for test infrastructure controllability and observability is the IEEE Std. 1687 [66]. It deals with the great number of DfT structures and connects them serially via programmable segment insertion bits (SIBs) to a reconfigurable scan network (RSN) between the scan in (SI) and scan out (SO) ports. When the SIB of a DfT structure is opened, its test data register (TDR) becomes part of the RSN such that it is accessed from the SI port and its output is streamed to the SO port.

IEEE Std. 1687 was developed with digital ICs in mind. The standard for analog test access is the IEEE Std. 1149.4 [67] and dates from the 1990s. It proposes a test bus paradigm that is still used today, but it requires a minimum of two additional test pins which is too costly and often prohibitive as many designs are pin-limited. To this end, nowadays there is an IEEE working group extending IEEE Std. 1687 [68] to include properties demanded by analog ICs, such as periodic sampling. The envisioned test access standard will be compatible for both analog and digital IPs in a SoC connecting them onto a common test infrastructure.

The principle for connecting analog IPs to the common test infrastructure is proposed in [64]. An example is shown in Fig. 1, depicting two analog IPs and several digital IPs connected to a common scan path. For simplicity, the SIBs are not included. To be able to connect analog IPs to the test infrastructure it is required that analog test stimuli and analog test responses are first digitized. This is achieved by using on-chip Digital-to-Analog Converters (DACs) and ADCs, respectively, which could be shared among several analog IPs if these are tested sequentially and the voltage ranges are consistent. Four types of connections to the scan path are shown in Fig. 1 for analog IPs: (a) a DAC connecting an analog node inside the IP or the DfT structure, e.g., for forcing an analog test stimulus; (b) an ADC connecting an analog node inside the IP or the DfT structure, e.g., for monitoring a test response signal; (c) a direct connection to the DfT, e.g., for activating a digitally-controlled re-configuration scheme or embedded test instrument; and (d) a direct connection to the digital tuning knobs used for calibration. Fig. 1 shows for simplicity 3-bit data converters and 3-bit words controlling the tuning knobs and DfT structures, but in fact any TDR size can be accommodated into the scan path. It also shows a number of intervening or appended TDRs that connect digital IPs to the scan path, as well as the case where an analog signal inside an analog IP is digitized via the ADC and driven into a digital IP and the case where the output of a digital IP is converted via the DAC to analog and drives an analog

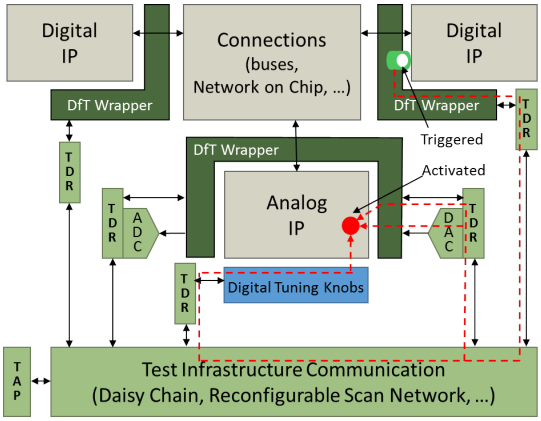


Fig. 2: HT scenario exploiting the SoC test infrastructure.

input of the analog IP. Finally, Fig. 1 shows the three main control signals, namely shift, update, and capture. The shift operation shifts the data serially through the scan path one bit per clock cycle. The update operation latches the data to the input of the ADC, to the input of the DfT structure, or to the programming bits of the tuning knobs. The capture operation offloads a digitized test response into the scan path to be scanned out for subsequent off-chip analysis. For each ADC and DAC, a counter and a packet size register are used that set the periodicity of the TDR update and capture operations. For a more detailed description of the test infrastructure, the interested reader is referred to [64].

VI. Proposed HT attack

A. Threat Model

We assume that the attacker has access to the SoC design and can manipulate a digital IP and the test infrastructure. The attacker also needs to have some minimum knowledge of the victim analog IP so as to design the HT payload. Based on this threat model, the attacker could be the SoC integrator or the foundry.

B. Attack scenario

It is well-known that the test infrastructure can be a vehicle for attacks. From a general point of view, such attacks can be categorized into external threats and internal threats. External threats consider an unauthorized user that gains control of the chip via the TAP. They include launching several types of scan attacks aiming at stealing secret keys [69], [70], performing reverse-engineering and device cloning [71], performing memory dumping [72], and modifying memory values to attain privilege escalation [73]. Internal threats consider that the attack takes place entirely inside the chip. For example, a third-party malicious IP connecting to the scan network can aim at sniffing confidential data or can act as a tampering IP corrupting the test data of another IP as they are being transported across the scan network [74]. For a more detailed description and a taxonomy of security threats in IEEE test standards, the interested reader is referred to [75].

In this paper, we propose a novel HT attack scenario where the test infrastructure is a vehicle for infecting an analog IP. The HT attack, illustrated in Fig. 2, exploits the fact that analog and digital IPs coexist in the SoC and are linked together via the shared common scan network, as described in Section V. The key characteristic of the proposed HT attack is that the HT is not hidden inside the analog IP itself, thus neither detection nor prevention are possible in the analog domain. Instead, the HT is well hidden inside a digital IP and the scan network. More specifically, the triggering mechanism is hidden inside a digital IP. Upon activation, the payload is generated and transported to the victim analog IP via the scan network. All the IPs apart from the targeted analog IP can be bypassed thanks to the programmability features of the RSN. The payload has two parts, a bit that opens a SIB of a DfT structure or the programmability interface of the analog IP, and a digital word that is a malicious test pattern applied to the input of the DfT structure or a malicious tuning knob setting. Essentially, during mission mode, the payload switches the analog IP in test mode or re-configures the analog IP in an undesired operation mode. It can be smartly designed so as to result either in performance degradation or denial-of-service for the analog IP. In fact, numerous malicious test patterns and tuning knob settings can serve this objective, and in practice it will suffice to activate just a single DfT structure controlled by few bits or change just one tuning knob value. In turn, if the analog IP controls other digital IPs, then the operation of the entire SoC can be jeopardized.

In Sections VII and VIII, we present two examples of how this scenario might play out in a SoC. In the first example, the HT infects an LDO via its DfT interface. Although the LDO is the direct victim of the HT, given that the LDO supplies one or more digital IPs inside the SoC, the HT infects implicitly other digital IPs too. In the second example, the HT infects an RF receiver via its programmability interface. In both examples, we design HT payloads that lead to performance degradation or denial-of-service.

C. HT design

The proposed HT attack scenario can make use of any triggering mechanism, i.e., combinational, sequential, or more complex triggering mechanisms, as discussed in the introduction. Several benchmark triggering mechanisms can be found in Trust-Hub [25]. For this reason, herein we do not cover in more detail this aspect of the HT design, and we will focus only on the payload mechanism aspects, by proposing several different examples.

The general payload mechanism consists in a malicious digital pattern applied at the interface of the analog IP during normal operation. In the case of infection via the DfT interface, the malicious pattern corresponds to an incorrect DfT pattern, either semi-activating or fully-activating the DfT structure, thus forcing the analog IP into either an incorrect test mode or the correct test mode. In the case of infection via the programming interface, the malicious pattern forces a malicious programming setting, either one that corresponds to a different operation mode or one that is invalid, i.e., not corresponding to any documented usage.

The result of unexpectedly activating the DfT or modifying the programming during normal operation can be either

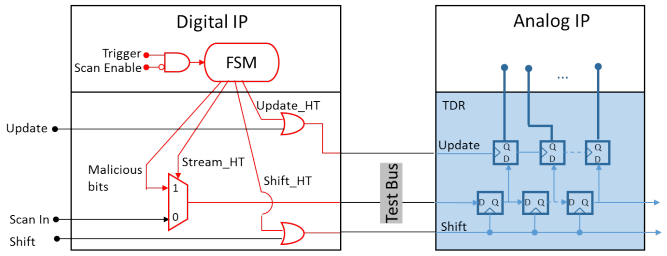


Fig. 3: Payload mechanism based on transporting the malicious bit pattern to the victim analog IP.

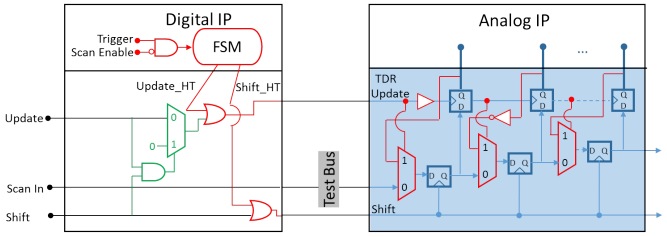


Fig. 4: Payload mechanism based on updating the TDR of the victim analog IP.

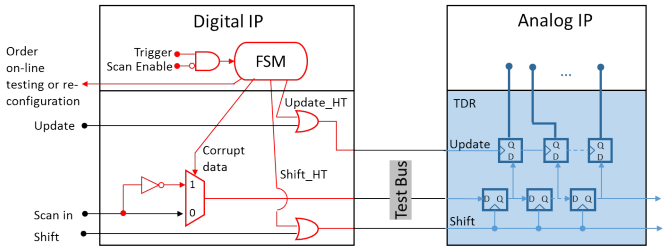


Fig. 5: Payload mechanism based on requesting on-line testing or re-configuration and subsequently corrupting the transported data.

performance degradation or denial-of-service. The malicious pattern is generated according to the attacker's objective. It can be simply generated by flipping bits in the DfT pattern that disables DfT or flipping bits of a given programming setting. Since the operation of analog circuits is very sensitive, flipping just one bit can lead to the desired effect for the attacker.

Fig. 3 shows a payload mechanism that generates the intent malicious pattern inside the digital IP and then transports it to the DfT or programming interface of the victim analog IP via the test bus. The HT design is shown in red color. Upon activation of the trigger, and only if the digital IP is not in test mode, i.e., the scan enable signal is 0, the malicious pattern is generated by a Finite State Machine (FSM), which also controls its transporting via the test bus. The trigger is suppressed during digital IP testing by using this AND gate so as to disable HT detection during testing. This point will be discussed in more detail in Section VI-D. The FSM sets signal $Stream\_HT$ to 1 to toggle the multiplexer and feed the malicious pattern into the test bus. Signal $Shift\_HT$ is also set to 1 to shift the malicious pattern downwards via the test bus for a number of clock cycles required to reach the victim analog IP. Then, signals $Stream\_HT$ and $Shift\_HT$ return to 0, and signal $Update\_HT$ is set to 1 to update the parallel data register of the TDR of the victim IP and force the malicious bit pattern.

Fig. 4 shows a payload mechanism that refreshes the parallel data register of the TDR of the victim IP while flipping a select set of bits to generate the malicious pattern. Prior to activation of the trigger, the parallel data register stores either the pattern that disables the DfT of the analog IP or a programming setting corresponding to a specific operation mode of the analog IP. Upon activation of the trigger, the FSM sets signals $Update\_HT$ and $Shift\_HT$ simultaneously to 1, which is not a valid condition during normal test mode. This generates the desired malicious pattern from the pattern stored in the parallel data register using inverters in appropriate positions, writes this malicious pattern into the serial shift register that is a segment of the scan chain, and updates the parallel data register writing into it the malicious pattern. A buffer is used in the update path to ensure that the write operation of the malicious pattern into the scan chain will be completed before the parallel data register is finally updated. Note that the pattern existing in the scan chain prior to the HT activation is a "don't care" pattern since the test bus is in idle mode during the payload application. Thus, altering this pattern is not an issue as it would have been eventually streamed off-chip and dumped.

Fig. 5 shows a third possibility where the payload mechanism requests on-line testing or re-configuration of the victim analog IP and corrupts the transported data as they pass by the scan network segment of the malicious digital IP. In this case, the attacker is aware of the geometry of the scan network and knows exactly the number of clock cycles needed for the data to reach the digital IP. At this point, the digital IP orders corrupting a select subset of bits in the data as they are being shifted to reach the victim analog IP.

A fourth scenario of payload mechanism could be the corruption of a test pattern or a programming setting stored in the memory. The memory re-write operation takes place upon activation of the HT, but the payload is applied later when the analog IP is subject to on-line testing or a re-configuration is demanded by the application.

D. Discussion on countermeasures

1) Countermeasures in the analog domain: The HT resides completely outside the analog IP and the payload is naturally applied to the analog IP via its DfT or programming interface. Thus, the HT is totally transparent to the analog IP and cannot be prevented or detected in the analog domain. Only the HT payload effect is shown in the analog domain after the HT is triggered in the digital domain when it is probably too late. Testing, statistical side-channel fingerprinting or destructive methods using reverse-engineering of the analog IP cannot reveal the presence of the HT. Thus, countermeasures against the proposed HT attack can only be implemented in the digital domain or via the test infrastructure itself.

2) Countermeasures in the digital domain: As already mentioned in Section VI-C, any trigger mechanism inside the "attacking" digital IP can be used in the context of the proposed HT attack scenario. Therefore, the proposed HT

attack can make use of any state-of-the-art stealthy and low footprint trigger. For this reason, the proposed HT attack can benefit from the most advanced trigger mechanisms at any point in time. We can consider that the stealthiness of the trigger against testing, statistical side-channel fingerprinting, run-time monitors, etc., can be as strong as that of the best trigger known.

Another important point is that no payload is seen by any of the digital IPs inside the SoC, including the attacking digital IP, since the payload is entirely directed to the victim analog IP. This means that several defenses that aim at detecting HTs by observing the digital IP outputs, i.e., testing by crafting test patterns to exercise the HT and propagate its effect to the output, are non-applicable.

On the other hand, analog and digital IPs are tested separately, meaning that during digital IP testing the SIB of the DfT or programming interface of the analog IP is closed. Therefore, even if the HT is exercised when test processes run on the digital IP, the payload will not be applied to the analog IP.

In the case where the HT is activated, however, the data in the scan chain will be polluted with the payload data possibly making this activity detectable once the data are streamed off-chip for analysis. To circumvent this, the attacker can place an AND gate after the trigger, controlled by the trigger and the digital IP inverse scan enable signals and driving the input of the FSM, as shown in Figs. 3-5. In this way, during digital IP testing the payload application to the analog IP is blocked and the streamed test data in the scan chain are not affected. This AND gate is not conflicting with the attack for any of the HT designs since it passes the trigger signal during normal operation of the digital IP.

Section VI-C described several payload mechanisms. These include a small FSM inside the attacking digital IP and few extra gates and MUXes in the scan chain, shown in red color in Figs. 3-5, so as to transport and generate the malicious pattern at the interface of the victim analog IP. Thus, the payload mechanism has a small footprint and can be effectively hidden inside the dense digital IP and the long scan chain of the test infrastructure.

Furthermore, all HT payload designs proposed in Section VI-C are transparent in normal test mode. Only the HT design in Fig. 4 can be detected with a test command that simultaneously sets the update and shift signals to 1. However, this test command can be easily suppressed by the attacker by placing a simple circuit acting on the update and shift signals in the segment of the scan chain corresponding to the attacking digital IP. This circuit, shown in green color in Fig. 4, is composed of an AND gate and a MUX. The update and shift signals are never simultaneously set to 1 during normal test operation. If such a test command occurs, the output of the AND gate is set to 1, thus setting the output of the MUX to 0 which flips the update signal from 1 to 0. In this way, when this test command is applied it is detected and suppressed before reaching the victim analog IP. As a result, neither the TDR of the victim analog IP is updated nor the data in the scan chain are corrupted. This is the expected behavior in HT-free operation, thus the HT goes undetected.

3) Countermeasures via the test infrastructure: There have been many recent works aiming at improving the trust in the test infrastructure, defending against the external and internal threats described in Section VI-B. A comprehensive overview and classification of such countermeasures can be found in [75]. Possible countermeasures include: (a) test infrastructure access authentication, e.g., by inserting a password inside the TAP controller [76] or implementing a challenge-response protocol [77], [78]; (b) scan network access authentication, e.g., by locking the SIB [79], implementing a challenge-response protocol [80], or obfuscating the geometry of the RSN structure [79], [81]; (c) privileged-based access restriction [78], which extends the access authentication techniques by assigning different privileges to the users according to the trust level they have; (d) assure data confidentiality, e.g., by test data encryption [74], [81] or isolating any untrusted instruments when confidential data are being shifted through the scan network [78]; (e) bidirectional IP block authentication, e.g., implementing a challenge-response protocol at the chip-level [74]; (f) assure data integrity [74], i.e., assure that the test patterns have not been modified during their transportation across the scan network; (g) on-line detection aiming at detecting the execution of the attacks while they are running, e.g., by setting rules to verify the test pattern compliance to a legitimate behavior [81]. The proposed HT attack is an internal threat and all the proposed HT designs are essentially tampering mechanisms corrupting test or programmability patterns. Countermeasures (a)-(c) defend against external threats only, thus the proposed HT attack can evade or bypass them, given also its insertion phase. Countermeasures (d)-(g) can defend against internal threats and the protection they can offer against the proposed HT attack should be evaluated. More specifically, data encryption cannot protect against the proposed HT designs since decrypting at the analog IP interface a randomly generated test or programmability pattern, or corrupting an encrypted test or programmability pattern by flipping many bits at random and subsequently applying it to the analog IP, will still infect the analog IP. The HT effect, however, will not be controllable by the attacker, and probably the HT will cause dramatic performance degradation or complete malfunction. Bidirectional IP block authentication and assuring data integrity can defend against the proposed HT attack, but they require significant extra on-chip resources, thus the overhead the defender has to pay is significant. On-line detection at the DfT or programming interface of the analog IP can be bypassed at the phase where the proposed HT is being inserted.

VII. Case Study: LDO

A. LDO regulator design

The LDO is one of the most popular power management systems to supply the sub-blocks of a SoC. It is a perfect target of a HT as the infection will spread to other IPs inside the SoC. We designed an LDO in the 65nm technology by STMicroelectronics using the free open-source OCEANE tool [82]. Its block-level schematic is shown in Fig. 6. It consists of a sub-band gap reference voltage generator (SBGR), an error amplifier implemented with an operational transconductance amplifier (OTA), a power p-MOS transistor, and a feedback

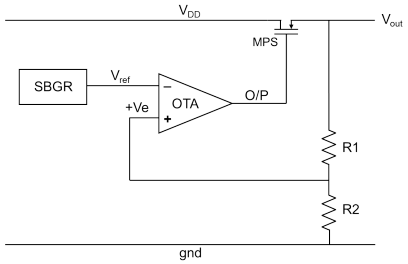


Fig. 6: Block-level schematic of the LDO.

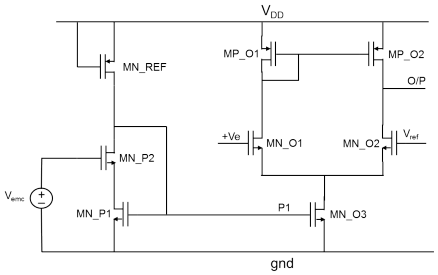


Fig. 7: Schematic of the error amplifier within the LDO implemented with an OTA.

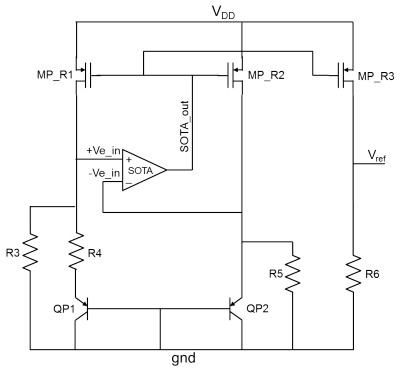


Fig. 8: Schematic of SBGR generator.

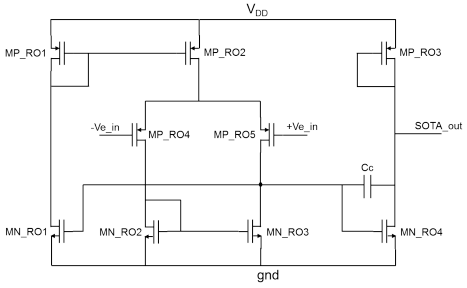


Fig. 9: Schematic of SOTA.

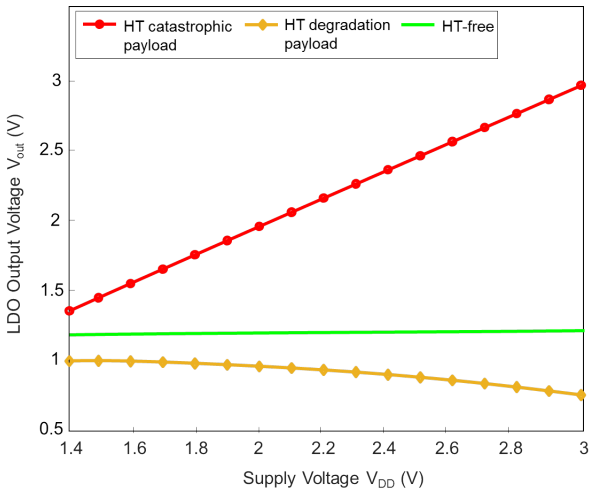


Fig. 10: LDO output variation as a function of power supply variation.

resistor network. The error amplifier monitors a fraction V_e of the LDO output voltage V_{out} through the resistor feedback network and compares it with the output voltage V_{ref} of the SBGR. If V_e is higher (lower) than V_{ref}, then the error amplifier drives the gate of the power transistor to decrease (increase) its output voltage so as to maintain a constant V_{out}. Figs. 7 and 8 show the schematics of the OTA and SBGR. Fig. 9 shows the schematic of the self-biased operational transconductance amplifier (SOTA) inside the SBGR.

The green curves in Figs. 10-12 show the nominal LDO performance in the HT-free scenario. Specifically, Fig. 10 shows the LDO output voltage V_{out} variation as a function of power supply voltage variations at 27^{o}C. V_{out} shows a 33.4mV variation when V_{dd} varies from 1.4V to 3V. Fig. 11 shows the LDO output dependence on temperature variations for a V_{dd} equal to 1.5V. V_{out} shows a 10mV variation when temperature varies from -55^{o}C to 125^{o}C. Fig. 12 shows the transient response of the LDO for a variation of load current from 50mA to 0mA and then from 0mA to 50mA, which corresponds to removing the load and then adding it back. The maximum overshoot is 44.9mV and settles after 875ns, while the maximum undershoot is 53.2mV and settles after 800ns.

B. DfT

We use a generic defect-oriented DfT technique proposed in [37]. The DfT principle is based on topology modification (or re-configuration) enabled by the addition of PD and PU transistors. A PD transistor connects a circuit node to ground, while a PU transistor connects a circuit node to the power supply. PD and PU transistors are activated by applying a logic 1 and 0 at their gates, respectively. If N PD and PU transistors are added, then the circuit can be configured into 2^N topologies, including the original one where all PD and PU transistors are deactivated. The underlying principle is that by these re-configurations we are able to expose the presence of additional defects that are undetectable in the original topology.

A DC test is used for the LDO. In particular, the LDO is self-activated and its output is used as the test output. In the defect-free case, for each test configuration, a different nominal test output value $V_{\text{test,j}}$ may be observed, where j denotes the configuration number. To account for process variations and avoid yield loss, we consider a tolerance window $\pm k * V_{\text{test,j}}$, $k > 0$. For the purpose of our experiment, we set $k = 0.1$.

The defect simulation is performed at transistor-level and

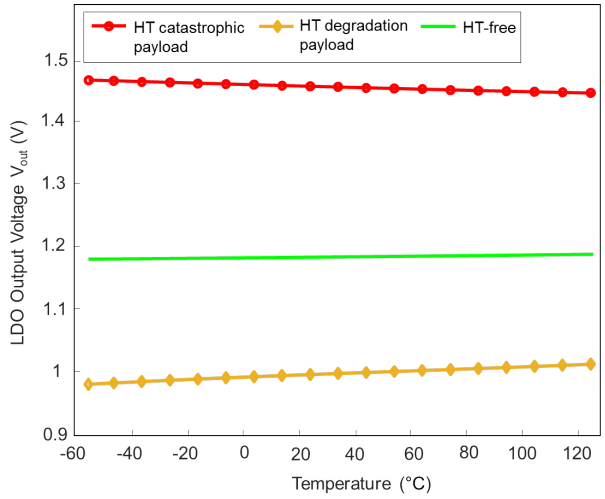


Fig. 11: LDO output variation as a function of temperature variation.

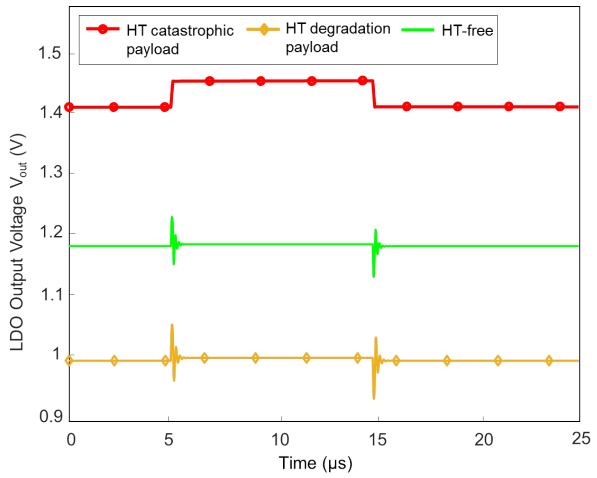


Fig. 12: Transient response of the LDO for a variation of load current.

in an automated workflow using the Tessent®DefectSim tool by Mentor®, A Siemens Business [83]. We cycle through all configurations and for each configuration defects are injected one by one. If $V_{\text{test,j}}$ is outside the tolerance window then the defect is deemed detectable by the test configuration.

We use the default defect model of the tool [83]. In particular, for MOS transistors we use only gate open and drain-to-source short defects. Similarly, for bipolar transistors, we consider base open and collector-emitter short defects. We consider the default short resistance of 10 ohms. Regarding opens, a weak pull-up or pull-down is assigned to each open defect to account for the facts that an ideal open does not exist and, besides, it cannot be handled by a SPICE simulator [83]. For passive elements, i.e., resistors and capacitors, we consider $\pm 50\%$ variations. In total, the defect model contains 60 defects. Furthermore, any of the N added PU or PD transistors could also contain defects, which increases the number of defects by $2N$. We consider the absolute defect coverage defined as the percentage of detected defects.

A defect coverage of 80% is reached using only the original topology. We applied the DfT technique considering that in a given re-configuration only one PU or PD transistor can be enabled. The LDO has 14 nodes in total, thus the number of possible re-configurations is 28. We performed an exhaustive search and we identified several nodes where PD and PU transistors can be added to result in a defect coverage of 100%. We kept a minimum set of 3 PD/PU transistors to reduce the DfT overhead at a minimum while maintaining the 100% defect coverage. The complete LDO schematic with the embedded DfT infrastructure composed of the 3 PU/PD transistors is shown in Fig. 13. One PD and one PU transistor, labelled by B1 and B2, respectively, are used inside the error amplifier, and one PD transistor, labeled by B3, is used inside the SBGR. The HT exploits this DfT infrastructure to stage the attack. The DfT is disabled with the pattern [B1,B2,B3]=010, while the patterns for enabling the three test configurations are [B1,B2,B3]=110, [B1,B2,B3]=000, and [B1,B2,B3]=011.

C. HT payload design

An interesting aspect of this DfT approach is that the DfT interface inside the LDO, i.e., transistors B1, B2, and B3, has a digital word input and can be connected directly to the scan network without using a DAC. Another interesting aspect specific to the LDO is that the LDO is self-driven without needing to specify an analog test input.

The HT payload consists in applying a malicious DfT pattern during normal operation. We identified two such DfT patterns that result in degradation of the LDO performance and to complete malfunction, respectively.

In particular, applying the DfT pattern [B1,B2,B3]=110 results in shifting the LDO output by about 15% and also results in small variation of the LDO output for temperature and V_{dd} variations, as shown by the orange curves in Figs. 10-12. In more detail, enabling B1 results in zero gate voltage for transistors MP_O1 and MP_O2 which increases the current flowing through them. However, the sum of the currents stays fixed since it equals the current flowing through MN_O3 which is fixed. As the voltages of all terminals of MP_O1 are fixed, it turns out that the current through MP_O2 reduces, which is enabled by the increase of the drain voltage of MP_O2. This voltage drives the gate of the power p-MOS transistor MPS and, thereby, the current that flows through MPS reduces, which reduces the LDO output. In turn, this reduces the voltage on the $+V_e$ terminal which points to reduction of the source voltage of MN_O1 since the current flowing through MP_O1 is fixed. This feedback effect reduces the drain voltage of MN_O2 which is the gate voltage of MPS. In the end, as it can be seen from Figs. 10-12, the LDO output settles at a slightly lower value of around 1V.

Applying the DfT pattern [B1,B2,B3]=011 results in a catastrophic effect in the operation of the LDO, as shown by the red curves in Figs. 10-12. In more detail, setting B3=1 connects the $+V_{e\_in}$ terminal of the SOTA to ground. The result is that V_{ref} follows V_{dd} instead of being stabilized at 0.7V. Since the output of the LDO follows V_{ref}, it shows a linear relationship with V_{dd} acting like a non-stabilized power supply. In addition, once the load is removed the response overshoots and never settles back unless the load is added again.

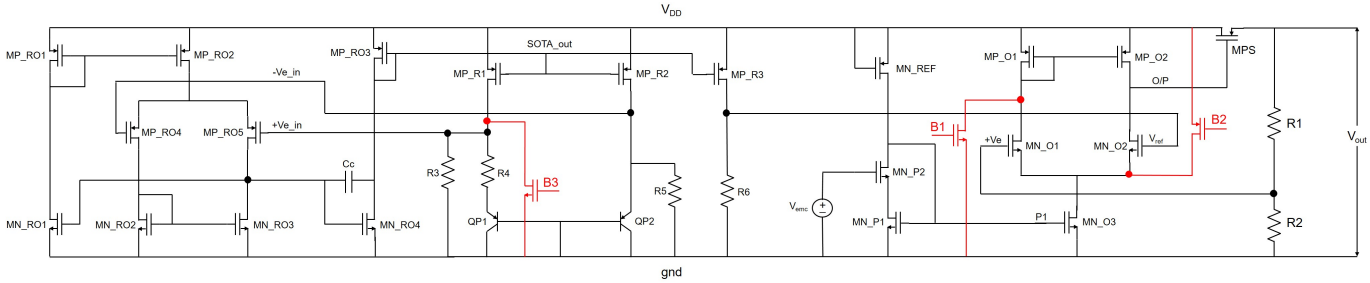


Fig. 13: LDO with DfT. The added PD and PU transistors to enable topology modifications are shown in red color.

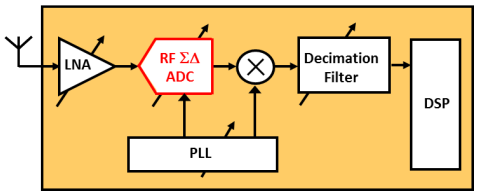


Fig. 14: Highly-digitized RF receiver architecture.

VIII. Case Study: RF Receiver

A. RF receiver programmable architecture

Our second case study is a programmable highly-digitized multi-standard RF receiver whose high-level architecture is illustrated in Fig. 14. A band-pass RF ΣΔ ADC is used to directly convert the RF signal at the output of the low noise amplifier (LNA) to the digital domain. The signal is then down-converted by a digital mixer and filtered using a digital decimation filter. The RF receiver is designed with programmable sub-blocks such that it can serve for establishing communication using several standards within the frequency range from 1.7 GHz to 2.8 GHz, including Bluetooth, ZigBee, WiFi 802.11b, etc. The programming aims at meeting the specifications of the target standard, i.e., sensitivity, center frequency, bandwidth, and resolution, while at the same time compensating for process variations and non-idealities so as to improve the overall performance trade-off. The designer uses a complex calibration algorithm to find appropriate programming settings that are unique per standard and per chip. The programmability is enabled by judiciously inserting digitally-controlled tuning knobs into the different sub-blocks.

The calibration is performed following testing/tuning iterations towards optimising the performance trade-off. The programming setting visited in each iteration is driven to the programmability interface via the scan network. For a given chip, once the calibration has been completed, the final matrix of the programming setting per standard is stored in an on-chip memory. During the application, when the programming setting is to be updated, the new programming setting is called from the associated memory address and driven to the RF receiver via the scan network where it is latched into the register of the programmability interface.

In our example, we infect the RF receiver via the modulator of the ΣΔ ADC. We rely on a recent design in the 65nm technology by STMicroelectronics [59] whose block-level architecture is illustrated in Fig. 15. The functionality of the modulator is adjusted using a 194-bit programming word. Fig. 15 shows the number of bits of the programming word controlling the operation of each sub-block.

Our experiment is conducted using hardware measurements on the actual fabricated chip. Without loss of generality, we consider that the RF receiver operates with center frequency 2.77GHz. The four main performances are plotted in Figs. 16, 17, 18, and 19. The green curves correspond to the nominal HT-free operation. More specifically, Fig. 16 shows the power spectral density (PSD) for an input power of -14dBm. The modulator has a nominal signal-to-noise ratio (SNR) of 60dB. Fig. 17 shows the SNR at different input power values with a step of 1dBm defining the dynamic range (DR) of the modulator. Fig. 18 shows the spurious-free dynamic range (SFDR) measured by applying two tones at the input with the same power and frequency difference of 2MHz. The modulator has a nominal SFDR of 51.39dB. Finally, Fig. 19 shows the output fundamental power and the third-order intermodulation (IM) product versus the input power, from which the input third-order intercept point (IP3) can be determined. The modulator has a nominal IP3 of 8dB.

B. HT payload design

The HT payload consists in unexpectedly altering the programming setting during normal operation. The issue here is that the final programming settings per operation mode and per chip are defined during testing time, while the HT is planted at an earlier phase. In other words, the matrix of final programming settings is unknown to the attacker and, in any case, will change from one chip to another. The attacker can still attain a controllable HT effect. The reason is that the programming setting is divided into segments each controlling a different sub-block, as shown in Fig. 15. Each segment of the programming setting can have one of two roles, namely either calibrating against process variations or setting the desired operation mode. Thus, for the HT to cause complete malfunction it suffices that it randomly flips bits in segments of the programming setting that are used for setting the operation mode. Accordingly, for the HT to cause performance degradation, it suffices that it randomly flips bits in segments of the programming setting that are used to calibrate against process variations. In fact, as we demonstrate below, in both scenarios it suffices that the HT flips just one bit in the nominal programming setting, which facilitates the HT payload design.

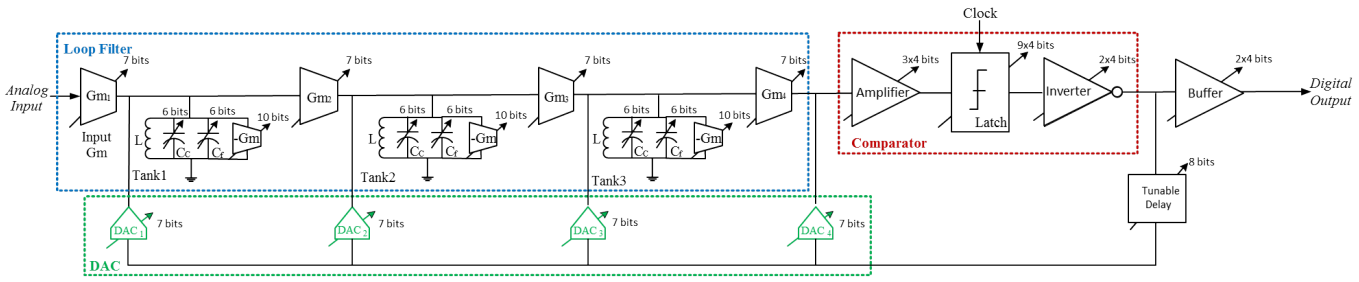


Fig. 15: Architecture of ΣΔ modulator.

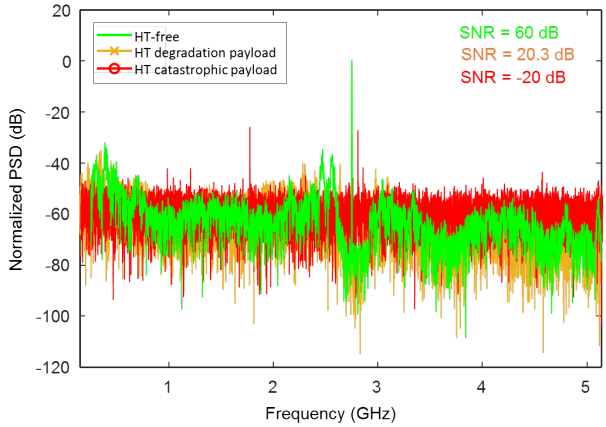


Fig. 16: PSD under HT-free and HT-infected operation.

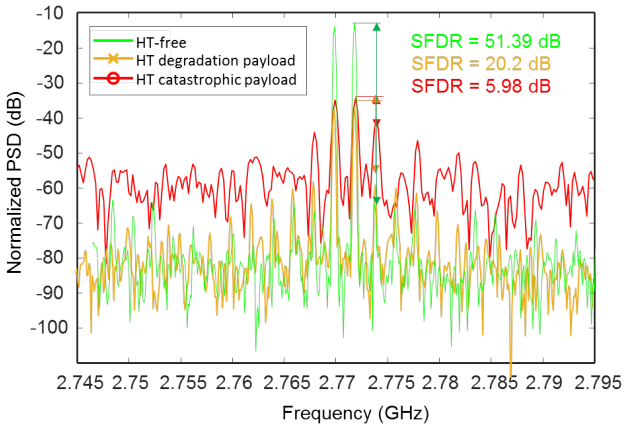


Fig. 18: SFDR under HT-free and HT-infected operation.

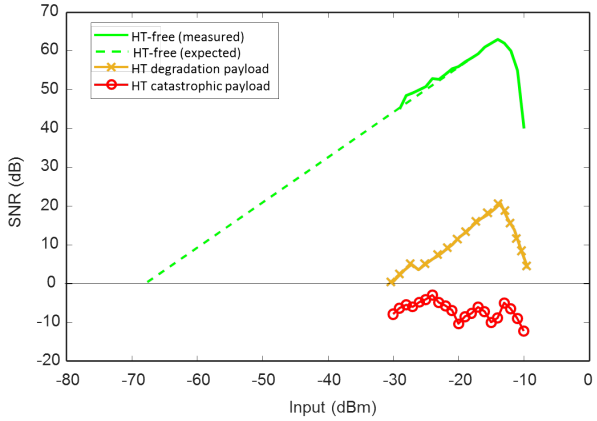


Fig. 17: Dynamic range under HT-free and HT-infected operation.

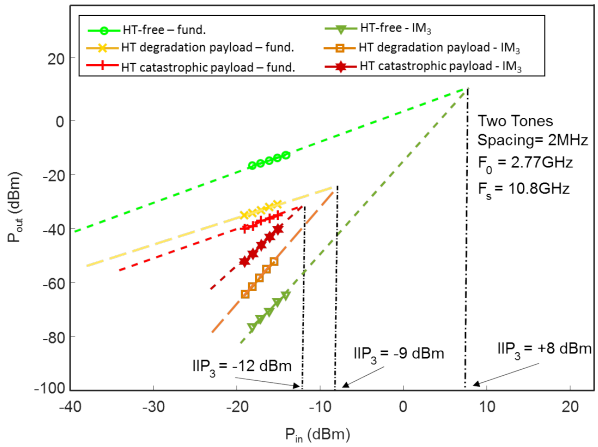


Fig. 19: IP3 under HT-free and HT-infected operation.

Returning to our case study, a candidate block where the HT can act to incite performance degradation is the negative transconductance -Gm in LC tank 1. The programmability of -Gm is responsible for improving the quality factor of the LC filter. Flipping one single bit in the programmability of -Gm will inevitably decrease the quality factor, thus untuning the RF receiver performance and degrading the SNR. The orange curves in Figs. 16-19 show the HT-infected performances in this scenario. As it can be seen, all performances are degraded.

A candidate block where the HT can act to incite complete malfunction is the tunable delay block in the feedback loop. The tunable delay block is responsible for controlling the center frequency of the noise shaping. It consists of delay elements and the programming connects or disconnects them so as to control the delay time. Flipping one bit in its programmming will inevitably set the RF receiver in another operation mode, most likely in an undocumented and invalid operation mode, thus leading to complete malfunction. The red curves in Figs. 16-19 show the HT-infected performances in this scenario. As it can be seen, there is no noise shaping and the signal now is buried under the noise floor.

IX. Conclusions

We proposed a novel HT attack scenario targeting infecting analog IPs embedded in a SoC. The HT lies in the dense

digital circuitry and transports its payload to the victim analog IP via the test bus. The payload consists of a malicious DfT pattern or programmability setting and is applied to the analog IP via the DfT circuitry or programmability fabric that are accessed via the test bus. We proposed different designs of the HT payload mechanism, while any HT trigger mechanism can be used in this context. The proposed HT attack was demonstrated on two case studies, namely an LDO regulator and an RF receiver. In the LDO case study, we considered an effective DfT approach and we derived malicious DfT patterns that can lead to performance degradation or denial-of-service. In the RF receiver case study, we demonstrated with hardware measurements that the infection can succeed by flipping only a select bit in the programming of the ADC that digitizes the received signal. The key characteristic of the proposed HT attack is that it is totally invisible in the analog domain, while it is stealthy and has a small footprint since the HT mechanism is hidden in its entirety into the digital part of the SoC.

REFERENCES

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

[2] K. Xiao, D. Forte, Y. Jin, R. Karri, S. Bhunia, and M. Tehranipoor, "Hardware Trojans: lessons learned after one decade of research," *ACM Transactions on Design Automation of Electronic Systems*, vol. 22, no. 1, pp. 6:1–6:23, 2016.

[3] Y. Shiyanovskii, F. Wolff, A. Rajendran, C. Papachristou, D. Weyer, and W. Clay, "Process reliability based trojans through NBTI and HCI effects," in *NASA/ESA Conference on Adaptive Hardware and Systems*, 2010, pp. 215–222.

[4] L. Lin, T. Güneysu M. Kasper, C. Paar, and W. Burleson, "Trojan side-channels: Lightweight hardware trojans through side-channel engineering," in *Cryptographic Hardware and Embedded Systems - CHES 2009*. 2009, pp. 382–395, Springer Berlin Heidelberg.

[5] G. T. Becker, F. Regazzoni, C. Paar, and W. P. Burleson, "Stealthy dopant-level hardware trojans: Extended version," *Journal of Cryptographic Engineering*, vol. 4, no. 1, pp. 19–31, 2014.

[6] K. Yang, M. Hicks, Q. Dong, T. Austin, and D. Sylvester, "A2: analog malicious hardware," in *Proc. IEEE Symposium on Security and Privacy*, 2016, pp. 18–37.

[7] X. Zhang and M. Tehranipoor, "Case study: Detecting hardware trojans in third-party digital IP cores," in *IEEE International Symposium on Hardware-Oriented Security and Trust*, 2011, pp. 67–70.

[8] R. S. Chakraborty, F. Wolff, S. Paul, C. Papachristou, and S. Bhunia, "MERO: A statistical approach for hardware trojan detection," in *Cryptographic Hardware and Embedded Systems - CHES 2009*. 2009, pp. 396–410, Springer Berlin Heidelberg.

[9] V. R. Surabhi, P. Krishnamurthy, H. Amrouch, K. Basu, J. Henkel, R. Karri, and F. Khorrami, "Hardware trojan detection using controlled circuit aging," *IEEE Access*, vol. 8, pp. 77415–77434, 2020.

[10] V. R. Surabhi, P. Krishnamurthy, H. Amrouch, J. Henkel, R. Karri, and F. Khorrami, "Exposing hardware trojans in embedded platforms via short-term aging," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 39, no. 11, pp. 3519–3530, 2020.

[11] 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 *IEEE Symposium on Security and Privacy*, 2010, pp. 159–172.

[12] K. Xiao, D. Forte, and M. Tehranipoor, "A novel built-in self-authentication technique to prevent inserting hardware trojans," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 33, no. 12, pp. 1778–1791, 2014.

[13] J. Leonhard, M. Yasin, S. Turk, M. Nabeel, M.-M. Louërat, R. Chotin-Avot, H. Aboushady, O. Sinanoglu, and H.-G. Stratigopoulos, "MixLock: Securing mixed-signal circuits via logic locking," in *Proc. Design, Automation & Test in Europe Conference*, 2019.

[14] N. Limaye, E. Kalligeros, N. Karousos, I. G. Karybali, and O. Sinanoglu, "Thwarting all logic locking attacks: Dishonest oracle with truly random logic locking," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 40, no. 9, pp. 1740–1753, 2021.

[15] J. Rajendran, M. Sam, O. Sinanoglu, and R. Karri, "Security analysis of integrated circuit camouflaging," in *Proc. ACM Conference on Computer and Communications Security*, 2013, pp. 709–720.

[16] J. Leonhard, A. Sayed, M. Louërat, H. Aboushady, and H. Stratigopoulos, "Analog and mixed-signal IC security via sizing camouflaging," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 40, no. 5, pp. 822–835, 2021.

[17] T. D. Perez and S. Pagliarini, "A survey on split manufacturing: Attacks, defenses, and challenges," *IEEE Access*, vol. 8, pp. 184013–184035, 2020.

[18] T. Sugawara, D. Suzuki, R. Fujii, S. Tawa, R. Hori, M. Shiozaki, and T. Fujino, "Reversing stealthy dopant-level circuits," *Journal of Cryptographic Engineering*, vol. 5, no. 2, pp. 85–94, 2015.

[19] B. Lippmann, M. Werner, N. Unverricht, A. Singla, P. Egger, A. Dübotzky, H. Gieser, M. Rasche, O. Kellermann, and H. Graeb, "Integrated flow for reverse engineering of nanoscale technologies," in *Proc. Asia and South Pacific Design Automation Conference*, 2019, p. 82–89.

[20] F. Stellari, P. Song, A. J. Weger, J. Culp, A. Herbert, and D. Pfeiffer, "Verification of untrusted chips using trusted layout and emission measurements," in *IEEE International Symposium on Hardware-Oriented Security and Trust*, 2014, pp. 19–24.

[21] D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi, and B. Sunar, "Trojan detection using IC fingerprinting," in *IEEE Symposium on Security and Privacy*, 2007, pp. 296–310.

[22] Y. Jin and Y. Makris, "Hardware trojan detection using path delay fingerprint," in *IEEE International Workshop on Hardware-Oriented Security and Trust*, 2008, pp. 51–57.

[23] S. Narasimhan, W. Yueh, X. Wang, S. Mukhopadhyay, and S. Bhunia, "Improving IC security against trojan attacks through integration of security monitors," *IEEE Design & Test of Computers*, vol. 29, no. 5, pp. 37–46, 2012.

[24] D. Forte, C. Bao, and A. Srivastava, "Temperature tracking: An innovative run-time approach for hardware trojan detection," in *IEEE/ACM International Conference on Computer-Aided Design*, 2013, pp. 532–539.

[25] B. Shakya, T. He, H. Salmani, D. Forte, S. Bhunia, and M. Tehranipoor, "Benchmarking of hardware trojans and maliciously affected circuits," *Journal of Hardware and Systems Security*, vol. 1, no. 1, pp. 85–102, 2017.

[26] Y. Jin and Y. Makris, "Hardware trojans in wireless cryptographic ICs," *IEEE Design & Test of Computers*, vol. 27, no. 1, pp. 26–35, 2010.

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

[28] S. Chang, G. Bhat, U. Ogras, B. Bakkaloglu, and S. Ozev, "Detection mechanisms for unauthorized wireless transmissions," *ACM Transactions on Design Automation of Electronic Systems*, vol. 23, no. 6, pp. 70:1–70:21, 2018.

[29] K. S. Subramani, N. Helal, A. Antonopoulos, A. Nosratinia, and Y. Makris, "Amplitude-modulating analog/RF hardware trojans in wireless networks: Risks and remedies," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 3497–3510, 2020.

[30] Z. Liu, Y. Li, Y. Duan, R. L. Geiger, and D. Chen, "Identification and break of positive feedback loops in trojan states vulnerable circuits," in *Proc. IEEE International Symposium on Circuits and Systems*, 2014, pp. 289–292.

[31] X. Cao, Q. Wang, R. L. Geiger, and D. J. Chen, "A hardware trojan embedded in the inverse widlar reference generator," in *Proc. IEEE International Midwest Symposium on Circuits and Systems*, 2015.

[32] Q. Wang, R. L. Geiger, and D. Chen, "Hardware trojans embedded in the dynamic operation of analog and mixed-signal circuits," in *Proc. National Aerospace and Electronics Conference*, 2015, pp. 155–158.

[33] C. Cai and D. Chen, "Performance enhancement induced trojan states in op-amps, their detection and removal," in *Proc. IEEE International Symposium on Circuits and Systems*, 2015, pp. 3020–3023.

[34] Q. Wang, D. Chen, and R. L. Geiger, "Transparent side channel trigger mechanism on analog circuits with PAAST hardware trojans," in *IEEE International Symposium on Circuits and Systems*, 2018.

[35] M. Elshamy, G. Di Natale, A. Pavlidis, M. Louërat, and H. Stratigopoulos, "Hardware trojan attacks in analog/mixed-signal ICs via the test access mechanism," in *IEEE European Test Symposium*, 2020.

[36] G. Huertas, D. Vázquez, E. J. Peralías, A. Rueda, and J. L. Huertas, "Testing mixed-signal cores: A practical oscillation-based test in an analog macrocell," *IEEE Design & Test of Computers*, vol. 19, no. 6, pp. 73–82, 2002.

[37] A. Coyette, B. Esen, W. Dobbelaere, R. Vanhooren, and G. Gielen, "Automatic generation of test infrastructures for analog integrated circuits by controllability and observability co-optimization," *Integration, the VLSI Journal*, vol. 55, pp. 393–400, 2016.

[38] A. Pavlidis, M. M. Louërat, E. Faehn, A. Kumar, and H. G. Stratigopoulos, "*SymBIST*: Symmetry-based analog and mixed-signal built-in self-test for functional safety," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 68, no. 6, pp. 2580–2593, 2021.

[39] A. Chatterjee, "Concurrent error detection and fault-tolerance in linear analog circuits using continuous checksums," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 1, no. 2, pp. 138–150, 1993.

[40] H.-G. D. Stratigopoulos and Y. Makris, "Concurrent detection of erroneous responses in linear analog circuits," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 25, no. 5, pp. 878–891, 2006.

[41] G. Renaud, M. Diallo, M. J. Barragan, and S. Mir, "Fully differential 4-V output range 14.5-ENOB stepwise ramp stimulus generator for on-chip static linearity test of ADCs," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 27, no. 2, pp. 281–293, 2019.

[42] F. Azais, S. Bernard, Y. Bertrand, and M. Renovell, "Optimizing sinusoidal histogram test for low cost ADC BIST," *Journal of Electronic Testing: Theory and Applications*, vol. 17, no. 3-4, pp. 255–266, 2001.

[43] A. Laraba, H.-G. Stratigopoulos, S. Mir, and H. Naudet, "Exploiting pipeline ADC properties for a reduced-code linearity test technique," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 62, no. 10, pp. 2391–2400, 2015.

[44] T. Chen, X. Jin, R. L. Geiger, and D. Chen, "USER-SMILE: Ultrafast stimulus error removal and segmented model identification of linearity errors for ADC built-in self-test," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 65, no. 7, pp. 2059–2069, 2018.

[45] B. Dufort and G. W. Roberts, "On-chip analog signal generation for mixed-signal built-in self-test," *IEEE Journal of Solid-State Circuits*, vol. 34, no. 3, pp. 318–30, 1999.

[46] H. Malloug, M. J. Barragan, and S. Mir, "Practical harmonic cancellation techniques for the on-chip implementation of sinusoidal signal generators for mixed-signal BIST applications," *Journal of Electronic Testing: Theory and Applications*, vol. 34, no. 3, pp. 263–279, 2018.

[47] M. Barragan, R. Alhakim, H.-G. Stratigopoulos, M. Dubois, S. Mir, H. Le Gall, N. Bhargava, and A. Bal, "A fully-digital BIST wrapper based on ternary test stimuli for the dynamic test of a 40nm CMOS 18-bit stereo audio $\Sigma\Delta$ ADC," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 63, no. 11, pp. 1876–1888, 2016.

[48] H. Chauhan, Y. Choi, M. Onabajo, I.-S. Jung, and Y.-B. Kim, "Accurate and efficient on-chip spectral analysis for built-in testing and calibration approaches," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 22, no. 3, pp. 49 –506, 2014.

[49] S. Sunter and A. Roy, "On-chip digital jitter measurement, from megahertz to gigahertz," *IEEE Design & Test of Computers*, vol. 21, no. 4, pp. 314–321, 2004.

[50] H. Le-Gall, R. Alhakim, M. Valka, S. Mir, H. Stratigopoulos, and E. Simeu, "High frequency jitter estimator for SoCs," in *IEEE European Test Symposium*, 2015.

[51] M. Ince, E. Yilmaz, W. Fu, J. Park, K. Nagaraj, L. Winemberg, and S. Ozev, "Digital built-in self-test for phased locked loops to enable fault detection," in *IEEE European Test Symposium*, 2019.

[52] A. Valdes-Garcia, J. Silva-Martinez, and E. Sanchez-Sinencio, "On-chip testing techniques for RF wireless transceivers," *IEEE Design & Test of Computers*, vol. 23, no. 4, pp. 268–277, 2006.

[53] E. S. Erdogan and S. Ozev, "Detailed characterization of transceiver parameters through loop-back-based BiST," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 18, no. 6, pp. 901–911, 2010.

[54] M. Cimino, H. Lapuyade, Y. Deval, T. Taris, and J.-B. Bégueret, "Design of a 0.9V 2.45 GHz self-testable and reliability-enhanced CMOS LNA," *IEEE Journal of Solid-State Circuits*, vol. 43, no. 5, pp. 1187–1194, 2008.

[55] Y.-C. Huang, H.-H. Hsieh, and L.-H. Lu, "A built-in self-test technique for RF low-noise amplifiers," *IEEE Transactions on Microwave Theory and Techniques*, vol. 56, no. 2, pp. 1035–1042, 2008.

[56] L. Abdallah, H.-G. Stratigopoulos, S. Mir, and J. Altet, "Defect-oriented non-intrusive RF test using on-chip temperature sensors," in *Proc. IEEE VLSI Test Symposium*, 2013.

[57] L. Abdallah, H.-G. Stratigopoulos, S. Mir, and C. Kelma, "Experiences with non-intrusive sensors for RF built-in test," in *Proc. IEEE International Test Conference*, 2012, Paper 17.1.

[58] S. Li, J. Li, X. Gu, H. Wang, C. Li, J. Wu, and M. Tang, "Reconfigurable All-Band RF CMOS Transceiver for GPS/GLONASS/Galileo/Beidou With Digitally Assisted Calibration," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 23, no. 9, pp. 1814–1827, 2015.

[59] A. Sayed, T. Badran, M. Louërat, and H. Aboushady, "A 1.5-to-3.0GHz tunable RF sigma-delta ADC with a fixed set of coefficients and a programmable loop delay," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 67, no. 9, pp. 1559–1563, 2020.

[60] M. Andraud, H.-G. Stratigopoulos, and E. Simeu, "One-shot non-intrusive calibration against process variations for analog/RF circuits," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 63, no. 11, pp. 2022–2035, 2016.

[61] A. Antonopoulos, G. Volanis, Y. Lu, and Y. Makris, "Post-production calibration of analog/RF ICs: Recent developments and a fully integrated solution," in *International Conference on Synthesis, Modeling, Analysis and Simulation Methods and Applications to Circuit Design*, 2019, pp. 77–80.

[62] C. Maxey, G. Creech, S. Raman, J. Rockway, K. Groves, T. Quach, L. Orlando, and A. Mattamana, "Mixed-signal SoCs with in situ self-healing circuitry," *IEEE Design & Test of Computers*, vol. 29, no. 6, pp. 27–39, 2012.

[63] S. Lee, C. Shi, J. Wang, A. Sanabria, H. Osman, J. Hu, and E. Sánchez-Sinencio, "A built-in self-test and *In Situ* analog circuit optimization platform," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 65, no. 10, pp. 3445–3458, 2018.

[64] S. Sunter, J.-F. Côté, and J. Rearick, "Streaming access to ADCs and DACs for mixed-signal ATPG," *IEEE Design & Test*, vol. 33, no. 6, pp. 38–45, 2016.

[65] M. Portolan, "Automated testing flow: The present and the future," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 39, no. 10, pp. 2952–2963, 2020.

[66] "IEEE standard for access and control of instrumentation embedded within a semiconductor device," *IEEE Std 1687-2014*, 2014.

[67] "IEEE standard for a mixed-signal test bus," *IEEE Std 1149.4-2010 (Revision of IEEE Std 1149.4-1999)*, 2011.

[68] "IEEE standard for describing analog test access and control, https://standards.ieee.org/project/1687_2.html," *IEEE Std P1687.2*.

[69] B. Yang, K. Wu, and R. Karri, "Secure scan: A design-for-test architecture for crypto chips," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 25, no. 10, pp. 2287–2293, 2006.

[70] J. Da Rolt, G. Di Natale, M. Flottes, and B. Rouzeyre, "New security threats against chips containing scan chain structures," in *IEEE International Symposium on Hardware-Oriented Security and Trust*, 2011.

[71] L. Azriel, R. Ginosar, and A. Mendelson, "Revealing on-chip proprietary security functions with scan side channel based reverse engineering," in *Proc. Great Lakes Symposium on VLSI*, 2017, p. 233–238.

[72] Ing. M.F. Breeuwsma, "Forensic imaging of embedded systems using JTAG (boundary-scan)," *Digital Investigation*, vol. 3, no. 1, pp. 32–42, 2006.

[73] F. Majeric, B. Gonzalvo, and L. Bossuet, "JTAG combined attack - another approach for fault injection," in *IFIP International Conference on New Technologies, Mobility and Security*, 2016, pp. 1–5.

[74] K. Rosenfeld and R. Karri, "Attacks and defenses for JTAG," *IEEE Design Test of Computers*, vol. 27, no. 1, pp. 36–47, 2010.

[75] E. Valea, M. Da Silva, G. Di Natale, M.-L. Flottes, and B. Rouzeyre, "A survey on security threats and countermeasures in IEEE test standards," *IEEE Design & Test*, vol. 36, no. 3, pp. 95–116, 2019.

[76] F. Novak and A. Biasizzo, "Security extension for IEEE std 1149.1.," *Journal of Electronic Testing*, vol. 22, pp. 301–303, 2006.

[77] A. Das, J. D. Rolt, S. Ghosh, S. Seys, S. Dupuis, G. D. Natale, M.-L. Flottes, B. Rouzeyre, and I. Verbauwhede, "Secure JTAG implementation using schnorr protocol," *Journal of Electronic Testing*, vol. 29, pp. 193–209, 2013.

[78] R. Baranowski, M. A. Kochte, and H. Wunderlich, "Fine-grained access management in reconfigurable scan networks," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 34, no. 6, pp. 937–946, 2015.

[79] J. Dworak, A. Crouch, J. Potter, A. Zygmontowicz, and M. Thornton, "Don't forget to lock your SIB: hiding instruments using P1687," in *IEEE International Test Conference*, 2013.

[80] C. Clark, "Anti-tamper JTAG TAP design enables DRM to JTAG registers and P1687 on-chip instruments," in *IEEE International Symposium on Hardware-Oriented Security and Trust*, 2010, pp. 19–24.

[81] S. Kan, J. Dworak, and J. G. Dunham, "Echeloned IJTAG data protection," in *IEEE Asian Hardware-Oriented Security and Trust*, 2016.
[82] J. Porte, "Outil pour la conception et l'enseignement d'électronique analogique (OCEANE)," https://www-soc.lip6.fr/equipe-cian/logiciels/oceane/, Online.
[83] S. Sunter, K. Jurga, and A. Laidler, "Using mixed-signal defect simulation to close the loop between design and test," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 63, no. 12, pp. 2313–2322, 2016.

Mohamed Elshamy received the M.Sc. degree in Electronics and Communications Engineering from Cairo University, Giza, Egypt, in 2015 and the Ph.D degree from Sorbonne Université, Paris, France, in 2021. He is currently a research assistant in the laboratory of nanotechnology application in electronics at the Electronics Research Institute, Cairo, Egypt. His research interests include hardware security, analog and mixed-signal circuits, nano-electronics, and memristors.

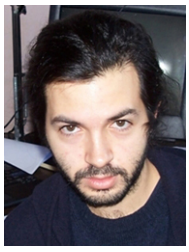
Giorgio Di Natale (Senior Member, IEEE) received the PhD in Computer Engineering from the Politecnico di Torino in 2003. He works as Director of Research for the French National Research Center (CNRS), and he is the director of the TIMA laboratory in Grenoble. His research interests include hardware security and trust, secure circuits design and test, reliability evaluation and fault tolerance, software implemented hardware fault tolerance, and VLSI testing. He serves as chair of the IEEE Computer Society TTTC from 2020, he is Golden Core member of the Computer Society and Senior member of the IEEE.

Alhassan Sayed received the B.Sc. and the M.Sc. degrees in Electrical Engineering, from the Electronics and Communications Department, Minia University, Minia, Egypt, in 2007 and 2010, respectively. He obtained his Ph.D. degree in Electrical Engineering and Computer Science from Sorbonne University, Paris, France, in 2016. He also spent 2 years (2017-2019) in a postdoctoral research position at the same University. Dr. Sayed is currently an Assistant Professor at Minia University, Minia, Egypt. His research interests include Sigma-Delta modulation, analog and RF circuit design, Analog-to-Digital conversion, and low noise amplifiers.

Antonios Pavlidis received the Diploma in electrical and computer engineering from the Aristotle University of Thessaloniki, Thessaloniki, Greece, in 2017, and the Ph.D. degree from the Sorbonne Université, Paris, France, in 2021. He is currently a Post-doctoral Researcher with the Laboratoire d'Informatique de Paris 6 (LIP6) at Sorbonne Université. His research interests include analog and mixed signal (AMS) circuits testing, Built-in-self-test (BIST) and Design-for-Test (DfT) for AMS circuits, fault diagnosis techniques for AMS circuits, Analog-to-Digital Converters (ADCs), machine learning, and hardware security.

Marie-Minerve Louërat received the M.Sc. degree in Electrical Engineering and the Ph.D. degree from Université Paris Sud, Orsay, France, in 1983 and 1986 respectively. In 1986 she joined the Centre National de la Recherche Scientifique (CNRS), France. She started at Fluids, Automation and Thermal Systems Laboratory, Université Paris Sud-CNRS, while teaching electronics. In 1992, she moved to the Computer Science Laboratory (LIP6), University Pierre et Marie Curie (now Sorbonne Université)-CNRS, France, while teaching VLSI. Between 2013 and 2018, she was the head of the System on Chip Department at LIP6. Dr. Louërat's research interest is electronic design automation methods and tools for analogue and mixed-signal circuits and systems. Most of her research activities have been supported by contracts, through academic and industrial cooperative projects in the framework of the FP7, Eureka/MEDEA, Catrene, Penta, and H2020 Projects. She published papers on static timing analysis, analogue and AMS design automation, analogue-to-digital converters, AMS system modelling and simulation, and test and security of AMS circuits and systems. She is a member of the AMS Working Group of Accellera Systems Initiative and contributed to standardize the AMS extension of SystemC since 2010. She has served on the Technical Program Committee of Design, Automation, and Test in European Conference (DATE) and several others international conferences. She co-chaired the Free Silicon Conference (FSIC) in 2019, Paris, France.

Hassan Aboushady (Senior Member, IEEE) received the B.Sc. degree in Electrical Engineering from Cairo University, Egypt, in 1993, the M.Sc. and Ph.D. degrees in Electrical Engineering and Computer Science from Sorbonne University, Paris, France, in 1996 and 2002 respectively. Dr. Aboushady is currently an Associate Professor at Sorbonne University. His research interests include Sigma-Delta modulation, Analog/RF circuit design, Analog-to-Digital and Digital-to-Analog conversion, as well as Security in analog and mixed-signal circuits. He is the author and co-author of more than 70 publications in these areas. He is the recipient of the 2004 best paper award in the IEEE Design Automation and Test in Europe Conference, as well as the recipient and the co-recipient of the 2nd and the 3rd best student paper awards of the IEEE Midwest Symposium on Circuits and Systems in 2000 and 2003 respectively. Dr. Aboushady is an IEEE-CAS distinguished lecturer and a member of the IEEE Circuits and Systems for Communications Committee (CASCOM). He also served as an Associate Editor of the IEEE Transactions on Circuits and Systems II: Express Briefs.



Haralampos-G. Stratigopoulos (Member, IEEE) received the Diploma in electrical and computer engineering from the National Technical University of Athens, Athens, Greece, in 2001 and the Ph.D. in electrical engineering from Yale University, New Haven, USA, in 2006. He is a Research Director with the French National Center for Scientific Research (CNRS) at LIP6 Laboratory, Sorbonne Université, Paris, France. His main research interests are in the areas of design-for-test for analog, mixed-signal, RF circuits and systems, machine learning, hardware security, and neuromorphic computing. He was the General Chair of the 2015 IEEE International Mixed-Signal Testing Workshop (IMSTW) and the Program Chair of the 2017 IEEE European Test Symposium (ETS). He has served on the Technical Program Committees of Design, Automation, and Test in Europe Conference (DATE), Design Automation Conference (DAC), IEEE International Conference on Computer-Aided Design (ICCAD), IEEE European Test Symposium (ETS), IEEE International Test Conference (ITC), IEEE VLSI Test Symposium (VTS), and several others international conferences. He has served as an Associate Editor of IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on Circuits and Systems I: Regular Papers, IEEE Design & Test, and Springer Journal of Electronic Testing: Theory & Applications. He received the Best Paper Award in the 2009, 2012, and 2015 IEEE European Test Symposium (ETS).