Security and Trust in the Analog/Mixed-Signal/RF Domain: A Survey and a Perspective

Angelos Antonopoulos, Christiana Kapatsori and Yiorgos Makris
Department of Electrical and Computer Engineering, The University of Texas at Dallas, Richardson, TX 75080
Email: {aanton, cxk161430, yiorgos.makris}@utdallas.edu

***Abstract*—We summarize and present the available body of knowledge in trusted and secure design of analog/mixed-signal/radio frequency (RF) integrated circuits (ICs) and intellectual properties (IPs), covering both known vulnerabilities and available remedies. Furthermore, we discuss the limitations of the current state-of-the-art in this topic, highlight the concomitant risks, and suggest research directions and steps to be taken towards designing, fabricating and deploying trusted and secure analog/mixed-signal/RF circuits. More specifically, a comprehensive survey of the relevant literature is provided, organized around three themes: (i) hardware Trojans and Trojan states in analog/mixed-signal/RF ICs along with existing detection/prevention methods, (ii) analog/mixed-signal/RF IC/IP reverse engineering and counterfeiting, as well as techniques for proving authenticity and ownership, and (iii) limitations of existing methods in the analog/mixed-signal (AMS) and RF domain, focusing on the gaps that exist in our current understanding of this problem and potential directions towards filling them and mitigating the threats in AMS/RF ICs/IPs.**

I. Introduction

Due to a number of factors entailing time to market pressure, IP re-usability, and outsourced manufacturing and testing, compromising the IC supply chain for sensitive commercial and defense applications has become possible through hardware Trojan attacks, reverse engineering and counterfeiting. All are targeting critical industrial sectors, such as military, infrastructure, automotive and telecommunication applications. For example a Syrian radar failure to warn the military of the incoming Israeli attack due to a back-door in off-the-self microprocessors, which were used in the radar system, was reported in 2008 [1]. Another hidden back-door in a computer chip that could allow an attacker to control critical applications, such as navigation and flight control in a Boeing 787 was discovered in 2012 [2]. Counterfeit Cisco products, which were bought by military agencies and contractors, and electric power companies in the United States with a potential threat of gaining access to highly secure systems were also recorded [3]. In 2011, the US military bought 59,000 counterfeit chips from China destined for installation in critical defense systems [4]. Finally, Dell warned of a hardware Trojan in some of its server motherboards in 2010 [5]. While extensive research efforts have been expended over the last decade in understanding security threats, as well as in developing prevention and detection solutions in digital circuits [6]–[10], the topic remains largely unexplored for their AMS and RF counterparts. A recent effort in [11] focuses in threats and countermeasures in digital ICs and discusses their relevance with the AMS domain. Therein, however, the largest body of state-of-the-art in security and trust in the AMS/RF domain remains unexplored. Accordingly, in this work we summarize and present the existing, albeit limited work on known vulnerabilities and proposed remedies for AMS/RF ICs and IPs.

II. Hardware Trojans in AMS/RF ICs

AMS/RF ICs have become an appealing target for attackers due to a number of reasons. This mainly stems from the widespread use of analog functionality (i.e., physical interfaces, sensors, actuators, wireless communications, etc.) in most contemporary systems and the inherent interaction between the analog/RF and digital domain in order to sense, process and communicate sensitive information (e.g. financial, personal or medical data). Communication of such sensitive information between nodes is extensively performed over wireless public channels. As a result, wireless networks employing both digital and analog/RF circuitry have been the target of covert channel attacks most of which are staged in software and firmware. Beyond such attacks, a hardware Trojan targeting the baseband part of an 802.11a/g transmitter to leak sensitive information over the air was recently shown in [12]. To date, however, only a few groups have investigated and reported existing vulnerabilities in the AMS/RF circuitry of transceivers used in wireless networks. In the following Sections we summarize the existing exploitation examples of such vulnerabilities by hardware Trojans along with respective defensive mechanisms.

A. Hardware Trojan Attacks

1) Hardware Trojans in Wireless Cryptographic ICs: A hardware Trojan attack in a wireless cryptographic IC, specifically in an ultra-wideband (UWB) transmitter was demonstrated through silicon measurements in [13], [14]. The attack targets both the digital and analog/RF parts of the IC and its general principle is shown in Figure 1. The attack is quite simple to implement and can be staged in various phases of the IC supply chain, e.g., in the design or the fabrication level. On the digital side, the added hardware taps into the register that stores the 128-bit advanced-encryption standard (AES) key, in order to steal one bit at a time. The value of the stolen key bit is forwarded to the UWB transmitter, through which it is leaked by modulating the parameters of the wireless communication during transmission of one ciphertext bit. Overall, along with

978-1-5090-5457-2/17/$31.00 ©2017 IEEE

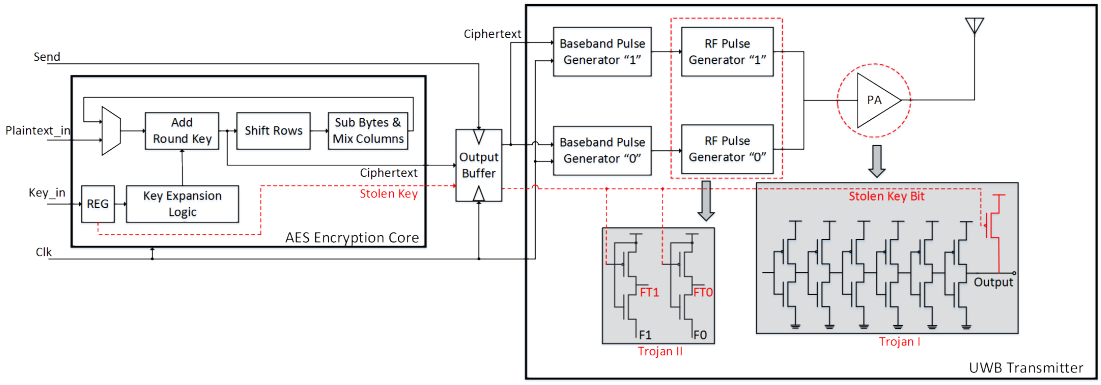

Fig. 1: Hardware Trojan modifications in digital and analog circuitry of a wireless cryptographic IC [13].

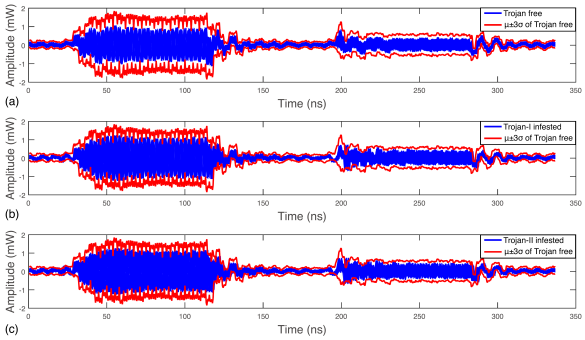

Fig. 2: Transmission power of 40 (a) Trojan-free ICs, (b) Trojan-I infested ICs, and (c) Trojan-II infested ICs enclosed in the $\mu \pm 3\sigma$ transmission [13].

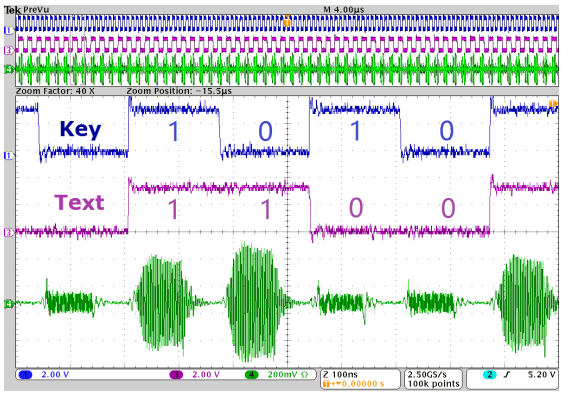

Fig. 3: Received waveform of a 4-bit ciphertext block transmitted by Trojan-I infested chip [13].

every 128-bit block transmitted by the UWB transmitter, the 128-bit key is also leaked [13].

Specifically, two hardware Trojans have been implemented on-chip, modulating the amplitude and frequency characteristics of the transmission. The first hardware Trojan, i.e., Trojan-I, which is modulating the amplitude, is implemented in the power amplifier (PA) and its overhead is very small, since it only demands one extra transistor to leak information. The key bit, which is forwarded through the digital part, is provided to the gate of the extra PMOS transistor. When the leaked key is "1", the transistor is off and, thus, the transmission power remains unaffected. However, when the leaked key bit is "0", the transistor turns on and adds a small current at the output node, thereby, slightly increasing the output power which is, in turn, passed to the antenna. On the other hand, Trojan-II, which is modulating frequency, adds two extra transistors at the inputs of each of the two RF pulse generators. Again, when the stolen key bit is "0" the PMOS transistor of Trojan-II in Figure 1 is turned on, thereby resulting in a higher frequency.

In order to investigate the Trojan impact on the legitimation and rogue transmission, the authors implemented 15 distinct Trojan levels [13]. Even for the maximum Trojan level, the Trojan impact on the legitimate transmission is carefully hidden in the transmission specification margins allowed for process variations. This is depicted in Figure 2, where the measured transmission power for transmitting a ciphertext bit of "0" and "1" for 40 Trojan free, 40 Trojan-I infested and 40 Trojan-II infested ICs is plotted versus time. For the Trojan infested transmissions, the maximum level of Trojan impact is employed. Each of the 3 distributions is enclosed in the $\mu \pm 3\sigma$ envelop of the Trojan-free ICs [13], [14]. Interestingly, none of the Trojan infested ICs falls out of the envelop boundaries.

Despite being hidden in the process variation margins, the impact of the hardware Trojan on the transmission power waveform suffices for the informed adversary to obtain the secret key and, by extension, the plaintext by deciphering the ciphertext. All the attacker has to do is listen to the public wireless transmission channel, focusing on the parameter manipulated by the hardware Trojan (i.e., amplitude or frequency), in order to observe the different levels, which correspond to a key bit of "1" and "0", respectively, when a ciphertext bit of value "0" and a ciphertext bit of value "1" are transmitted. This is shown in Figure 3 for a Trojan-I infested chip, where the receiver waveform of a 4-bit ciphertext block is illustrated. The minute amplitude increase when a key bit of "0" is transmitted - regardless of the text value - provides the attacker the information needed to correctly obtain the key. Similarly with Trojan-I, the attacker can also obtain the leaked information for the Trojan-II infested transmission [13], [14]. In both cases the receiver consists of an oscilloscope and an antenna connected on it.

2) RF Transmission Below Noise Floor: In line with [13], [14], the ability of hardware Trojans to hide unauthorized transmission signals within the ambient noise floor through the use of spread spectrum techniques was presented in [15]. The original concept of communicating with attackers below the noise power level was initially demonstrated in [16], where multi-bit information from a compromised crypto-processor was leaked through a power side-channel. Specifically, spread spectrum was used to distribute the power of side-channel leakage to multiple clock cycles, so that the signal-to-noise ratio (SNR) of each clock cycle is low enough to evade detection. The attacker can then exploit the side-channel information by averaging over a large number of clock cycles.

Similarly, the Trojan system in [15] spreads the rogue data and attenuates the Trojan signal so that it is pushed below the ambient noise floor. The principle of a spread-spectrum transmitter/receiver chain is shown in Figure 4. The low-rate baseband data is multiplied with a higher rate spread-spectrum code to generate a higher-rate sequence. The legitimate and Trojan spread signals are then added in the analog domain, constituting the signal to be transmitted, as shown in Figure 4. The transmitted signal, containing both the legitimate and rogue coefficients has an identical spectrum with the legitimate one, and thus the Trojan presence cannot be easily detected. This higher-bitrate digital sequence is then transmitted over the noisy channel, which may undergo multi-path fading and multiple interferers. At the receiver, both the useful signal and interferers are mixed with the same spread-spectrum code, de-spreading the original information, and spreading the interferers instead. Extremely low-power levels are required to retain effective communication. However, this comes at the cost of reduced throughput for the attacker. The spread-spectrum attack does not affect the legitimate transmission since it remains well hidden below the noise floor, thereby evading any performance-based testing or monitoring [15].

3) Hardware Trojans in AMS ICs: Unlike RF circuits, where a hardware Trojan adds extra circuitry to the legitimate structure to exploit its vulnerabilities, hardware Trojans in

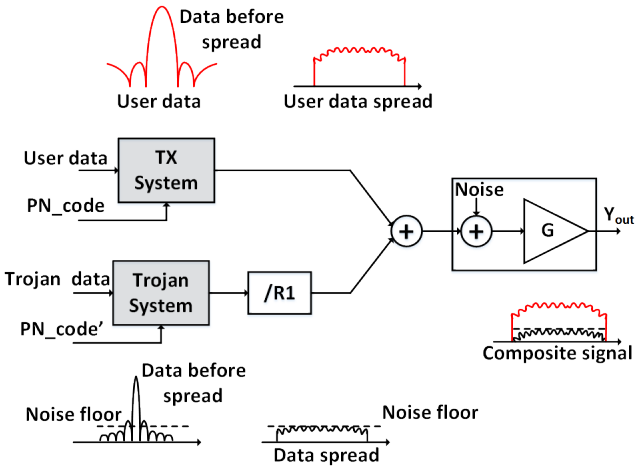

Fig. 4: Spread spectrum technique used for evading detection of hardware Trojans in wireless networks [15].

TABLE I: Trojan states in analog ICs

Reference	Circuit Topology	Simulation Level
[19], [20], [21]	Inverse Widlar	Cadence Spectre
[18], [22]	Filter	HSPICE
[23], [24]	Bandgap	Cadence Spectre
[25]	OP-AMP	Cadence Spectre
[22]	Wien-bridge oscillator	N/A

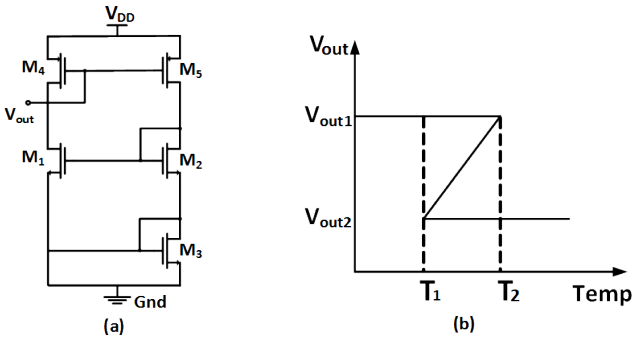

Fig. 5: (a) Schematic of the Inverse Widlar current mirror, and (b) multiple operating points in DC temperature sweep of the inverse Widlar current mirror. [21].

AMS ICs do not add extra overhead to the target IC, neither do they leave a signature during normal operation; rather, they exploit Trojan states that might be present in AMS components with positive feedback loops, which are commonly used to desensitize the circuit outputs from supply voltage variations. It all began back in 1980, when it was shown that transistor networks with positive feedback loops can have more than one solution to their DC equations, for some choice of network parameter values. In [17] it was reported that any circuit with positive feedback loops allows more than one DC operating points and, conversely, any circuit that has more than one solution in the DC equations must have positive feedback loops. These multiple DC operating points were demonstrated for verification purposes in a CMOS log-domain filter employing a positive feedback loop [18], but were never studied in the context of hardware security until recently. The problem of multiple operating states in analog circuits is commonly referred to as the start-up problem, meaning that a start-up circuit should typically be added to remove the undesired state. However, if no start-up circuit is used, which is quite common in analog design, or if the start-up circuit is infiltrated, a redundant state harboring a Trojan may still exist [19].

Several research results have shown that an AMS IC can exhibit a Trojan state, which can be defined as an operating state that forces the circuit to behave in an unexpected and undesired way, producing inconsistent results at its output, and, thus, directly affecting preceding blocks in a chain of IC components. These Trojan states have been shown to affect the output characteristics of operational amplifiers (OP-AMPs), current mirrors, bandgap references, oscillators and filters [19]–[22], [25], [26]. This has been verified via simulations performed in Matlab and Cadence Spectre, and results are

summarized in Table I.

In the Inverse Widlar current mirror shown in Figure 5(a), the output voltage may reach values other than the expected for a specific temperature, due to multiple equilibrium points [18], [21]. Indeed, as plotted in Figure 5(b), when temperature is swept, the same output voltage, V_{out2}, is obtained for temperatures T1 and T2. Similarly, a Trojan state was shown to exist in a fully differential operational amplifier when performance enhancement feedback, i.e. a slew-rate enhancement circuit, producing a positive feedback loop, is used [25]. Trojan states were also demonstrated via simulation results for a Wien-bridge oscillator [22]. These states occur when high non-linearities in the input-output characteristic are present. Specifically, the circuit may have either a static (undesired) or a dynamic mode of operation and, further, even when in dynamic mode, oscillation states of different amplitudes or frequencies may still occur, depending on the initial conditions of the capacitors [22]. Therefore, hardware Trojans in an oscillator can correspond either to a static mode, incapacitating the IC, or to unexpected oscillation characteristics, e.g. modified amplitude and frequency. Given the widespread use of oscillators in transceivers, a Trojan state could have devastating consequences, e.g., it could result in a shift of the local oscillator frequency to a different band, which an attacker could exploit to leak sensitive information.

This class of hardware Trojans does not demand any increase in power, area, or architecture and, thus, leaves no signature. Therefore, even if the complete circuit schematic is available, the presence of multiple operating points during design and verification can remain undetected.

B. Hardware Trojan Defenses

Traditional test methods are ineffective in detecting hardware Trojans: (i) with small overhead (in terms of area and power), (ii) which do not violate any protocol specifications, and (iii) which remain within the margins allowed for process variations. However, several defensive methods have been lately reported, capable of raising a red flag in the presence of hardware Trojans which manipulate transmission characteristics, similar to those previously described. These defensive mechanisms range from statistical side-channel fingerprinting to concurrent and formal methods, as discussed below.

1) Statistical Methods: Constructing IC fingerprints based on side-channel parameters and using these fingerprints to statistically assess whether an IC is contaminated by a hardware Trojan or not, was first presented in [27], [28] through a global power consumption-based and a delay-based method. The idea of side-channel fingerprinting is the basis for detecting the two hardware Trojans, which were presented in Section II-A1. The general principle, which was originally described in [10], [14], [29], relies on the systematic impact that hardware Trojans impose on transmission characteristics. This systematic impact is essential for the attacker to be able to discern the hidden information, as was shown in Figure 3. In practice, hardware Trojans add a statistical structure to the transmission characteristics, either in power, or in frequency, which is precisely

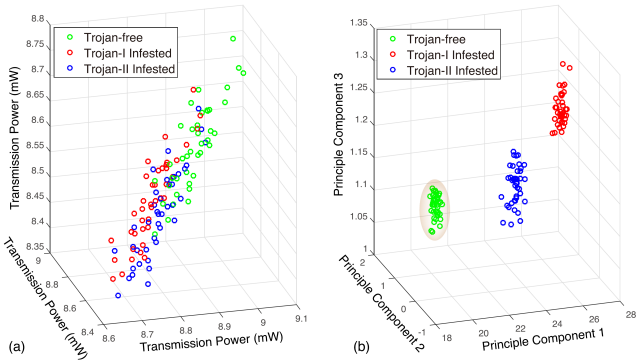

Fig. 6: Trojan-free and Trojan-infested circuits projected on a 3-D space where the populations: (a) are indistinguishable, and (b) can be distinguished after applying PCA [13].

what statistical side-channel fingerprinting exploits in order to uncover malicious operation.

To demonstrate the effectiveness of statistical side-channel fingerprinting, the authors in [10], [14], [29] performed the following experiment: Initially, the same six blocks of ciphetext were transmitted by the UWB RF front-end for each of the 40 Trojan-free, 40 Trojan-I infested and 40 Trojan-II infested ICs. Visualization of the accumulated transmission power in a 3-D space does not reveal any suspicious operation since all populations fall upon each other as depicted in Figure 6(a). However, when a simple statistical processing, such as principal component analysis (PCA) along with a one-class classifier is employed, the three populations become clearly distinguishable, as shown in Figure 6(b). Consequently, hardware Trojan activity can be detected.

A method for detecting the hardware Trojan of Section II-A2, as well as hardware Trojans in mobile platforms, was presented in [30]. This method does not require any golden reference; rather, it is based on self-referencing. In [30], the output of a mobile platform running on a commercial MpSoC board is driven into a periodic steady state (PSS) to decouple the response of the board from that of noise and Trojan. The changes in the circuit behavior between periods indicate the existence of unauthorized activity. After exciting the circuit and obtaining its current consumption signal, this signal passes through a low pass filter to obtain the self-referencing signal. This is then subtracted from the original signal to obtain a difference signal, which consists of noise and malicious activity, if any. Analysis of the difference signal in the time domain is not capable to distinguish the Trojan signal from channel noise. However, by using the fast Fourier transform of the difference signal, calculating the average noise level and setting a threshold of $3\sigma_n$ for noise referencing, where σ_n is the noise variance, the Trojan signal can be detected. Any unexpected bin (i.e., frequency bins that do not correspond to the fundamental and its harmonics) which is above threshold is considered a spectral violation. For demonstration purposes, the authors in [30] collected 240 data spectra, half of which were Trojan infested. For spectra without any Trojan activity the maximum number of extra

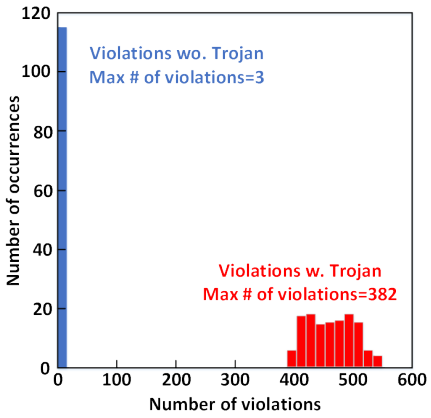

Fig. 7: Histogram of spectral violations for spectra with and without Trojan activity [30].

bins is 3, whereas the corresponding additional bins for the Trojan infested spectra is much greater, i.e., greater than 380 for all spectra. This is shown in Figure 7. Despite the Trojan operation at or below the noise level, its activity is clearly observable through the number of bin violations.

2) Concurrent Hardware Trojan Detection Method: Statistical side-channel fingerprinting methods operate either before an IC is deployed or, periodically, during idle times, after an IC is deployed. Therefore, they can be easily evaded by a hardware Trojan which remains dormant at all times except during normal operation. To counteract this issue, a concurrent hardware Trojan detection (CHTD) method which operates along with the normal functionality of the IC was presented in [31].

The method checks an invariant property of the circuit and uses an on-chip one-class classifier to assert a CHTD output when the invariance is violated. The classifier is trained using trusted side-channel fingerprints obtained at test time when the Trojan is dormant. The trained classifier can, then, be used to examine compliance of runtime observations of the invariant property, by comparing their footprint in the side-channel fingerprinting space to the learned boundary. To assess whether the invariant property is violated or not, two observations are collected from a single ciphertext bitstream transmission. Each of the observations consists of k bits, m of which are "1s". If the integrated voltage for observations A and B is V_A and V_B,

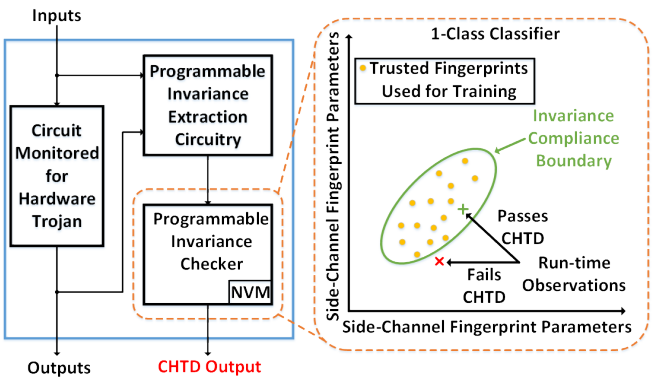

Fig. 8: CHTD experimentation platform [31].

respectively, then, the following invariance should always hold true:

$$|V_A(k,m) - V_B(k,m)| = \delta_{noise}, \quad (1)$$

where δ_{noise} represents noise measurements and non-idealities. If different k and m values are used for the two observations, the invariance becomes:

$$|V_A \cdot (k_A, m_A) - V_B \cdot (k_B, m_B)| = \delta_{noise} + |(m_A - m_B) \cdot V_{C1} + [(k_A - m_A) - (k_B - m_B) \cdot V_{C0}]|, \quad (2)$$

where V_{C1} and V_{C0} is the integrated voltage for a transmission of a bit equal to "1" and "0", respectively. Apart from its non-intrusive performance, CHTD is a self-referencing approach, which gives the flexibility of choosing different values for k_A, m_A, k_B, and m_B, thus making the design of a hardware Trojan which can evade the invariant property checking very difficult for an attacker. Effectiveness of the CHTD method was verified on the Trojan infested ICs of Section II-A1 and was demonstrated in [31].

3) Formal Methods: An information flow tracking (IFT) approach for ensuring data confidentiality in analog/RF designs was recently presented in [32]. The IFT was integrated into an automated proof-carrying hardware intellectual property (PCHIP)-based framework which was initially used to enforce information flow policies on digital designs. The proposed approach, which operates at the transistor level, converts the netlist of the analog/RF circuitry to a Verilog representation and, accordingly, uses an automated framework called *VeriCoq-IFT* to: (i) automatically convert the Verilog design to the Coq representation, (ii) generate security property theorems for preventing sensitive information leakage, and (iii) construct their proofs [32].

As demonstrated in [32], the method is able to detect sensitive data leakage from the digital domain to the analog domain and vice versa, without requiring any modification of the analog/mixed-signal/RF circuit design flow. This formal method was applied on the AES UWB tranmitter design of Section II-A1. Its Verilog netlist was extracted and the *Plaintext* and *Key* signals were annotated with appropriate sensitivity levels, as shown in Figure 9. The corresponding sensitivity was also marked, reducing operations in the AES core. Then, using *VeriCoq-IFT*, the design was converted to the formal representation and *Coq* was used to evaluate the proof for the security theorem asserting the sensitivity of the design output. In the Trojan-free case, the proof of the security property theorem for the output passes in *Coq*, attesting that this output never leaks sensitive information, under the provision that the initial sensitivity values and

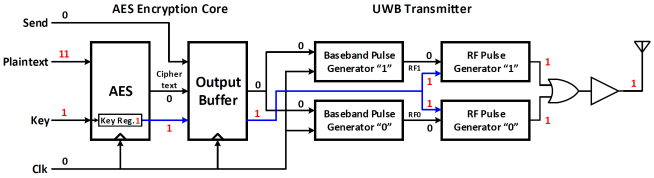

Fig. 9: Information leakage path in Trojan-II [32].

sensitivity-reducing operations were annotated correctly in the design. The effectiveness of the method was also verified in the presence of Trojan-I and Trojan-II, wherein the proof did not pass in *Coq*. This implies that a possible path exists, through which sensitive information may leak to the output. Figure 9 shows the information leakage path and the propagated signal sensitivity levels in the AES UWB design for Trojan-II.

4) Observation of Parasitic Loads: Detection of hardware Trojans which add some structure to the compromised IC was recently discussed in [33] for RF circuits. The method is based on the signature left due to rogue load capacitances. Specifically, stimulus optimization experiments were performed in a typical cascode low noise amplifier (LNA) and allowed detection of capacitive loads (due to the presence of hardware Trojans in the legitimate circuit) in several of the LNA's internal nodes.

5) Homotopy Methods: Defense mechanisms that have recently been applied for detecting multiple operating points in analog circuits with positive feedback loops are based in homotopy theory, which has been long used for verification purposes [34]. Given an analog circuit, the first step towards identifying Trojan states relies on determining the circuit's positive feedback loops. This is achieved by constructing a directed dependency graph based on its circuit topology. For example, in the bootstrapped V_t reference circuit of Figure 10(a), two feedback loops can be identified. These loops are:

$$I_1 \rightarrow B \rightarrow I_2 \rightarrow A \rightarrow I_1 \quad (3)$$

$$I_1 \rightarrow B \rightarrow I_2 \rightarrow C \rightarrow I_1 \quad (4)$$

Specifically, changes in current I_1 flowing through transistors M_4 and M_1 affect voltage at node B, which in turn pushes I_2 to change. Thereby, node voltage A is also affected, which accordingly, impacts I_1. Similarly, the second graph is described by Equation (4). Since only the positive feedback loops need to be identified, voltage/current dependencies are annotated with a sign. For example, an increase in the node voltage A results in a decrease in I_1, since A is applied to the gate of PMOS transistor M_4. Therefore the edge $A \rightarrow I_1$ in the top loop of Figure 10(c) receives a "$-$" sign. After all signs have been annotated, a positive feedback loop is defined as a feedback loop which contains an even number of negative dependencies, whereas a negative feedback loop contains an odd number of negative dependencies. Therefore, the feedback loop described by Equation (3) is a positive feedback loop [23], [24], [35], [36].

After the positive feedback loops have been identified, the continuation method can be applied to identify presence of multiple operating states. The method involves the introduction of a voltage or current source that can be swept to trace operating points of a circuit other than the desired and can be viewed as a homotopy approach applied to each positive feedback loop [37]. The most common approach in the continuation method involves insertion of sources that do not break any loops in the circuit, thereby circumventing concerns about

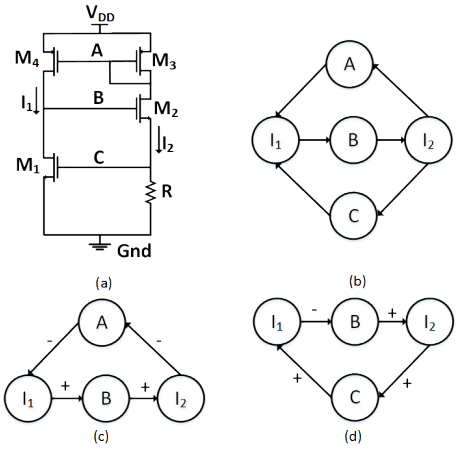

Fig. 10: Bootstrapped V_t reference circuit: (a) schematic, (b) directed dependency graphs, (c) dependence sign for the top loop, and (d) dependence sign for the bottom loop [23].

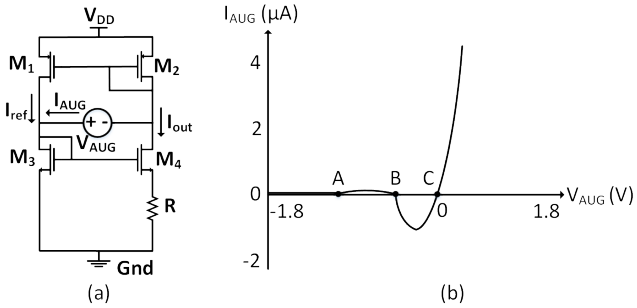

Fig. 11: (a) Constant g_m reference circuit and (b) I-V curve from the continuation method [38].

loop loading when a feedback loop is broken. Methods in which feedback loops are broken can also be used provided the operating points are not disturbed by breaking the loops [36], [37]. The continuation method has been demonstrated in several AMS ICs employing positive feedback loops [20], [23], [24], [26], [36], [37]. An example of the method is shown in Figure 11, where a voltage source, V_{AUG} is inserted in a constant g_m reference circuit. When this voltage source is swept the resulting current plot indicates three operating points labeled as A, B, and C. The right-most zero-crossing at point C is the desired one, since at this point $V_{AUG} = -0.2V$, which means that all transistors are biased in saturation [38], whereas operating points A and B correspond to undesired states.

A homotopy-type circuit simulation employing temperature sweeping can also raise a red flag for the circuit designer, as has been shown in [21].

Ad-hoc methods for preventing undesired states in analog ICs are also existent in the literature. Specifically, in [19] simulation results indicate that by decreasing the width of the diode-connected transistor M_3 in the Inverse Widlar current mirror of Figure 5(a), the region in which output voltages overlap, thus resulting in Trojan states, can be eliminated. Another route for detecting Trojan states in AMS circuits could be to use formal verification after AMS designs have

been approximated as purely Boolean models, as in [39], [40]. However, this has not been investigated so far. The same holds for [41], wherein a formal-based solution to the verification of AMS designs was applied in a delta-sigma modulator, validating its operation with respect to a given set of properties.

C. Analog Triggers

A key limitation of the AMS Trojan states which were previously presented stems from the lack of trigger mechanisms being capable of driving a circuit into an undesired state. So far, a few analog triggers have been presented in literature and are discussed below.

1) Capacitors: An analog trigger targeting a digital microprocessor was demonstrated in [42]. Similar to [16], where a capacitor of adjustable value is used to leak information conveyed by a power side-channel, the circuit in [42] employs capacitors to siphon charge from nearby wires as they transition between digital values. When the capacitors fully charge, an attack to a victim flip-flop is staged [42]. The capacitor performs analog integration of charge from a victim wire while at the same time being able to reset itself through charge leakage. Every time the victim wire toggles, the capacitor's charge increases and its voltage exceeds a predetermined threshold voltage. When the trigger input is inactive, the leakage current gradually reduces the capacitor's voltage and eventually stops the trigger output. Operation of the analog trigger is described in Figure 12.

2) Voltage glitches: Voltage glitches of the power supply is another trigger mechanism whose impact was shown on a

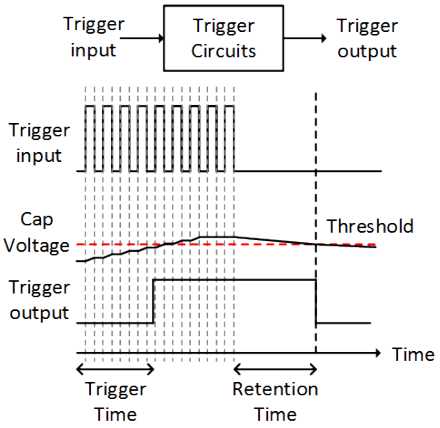

Fig. 12: Behavioral model of the capacitor-based analog trigger circuit [42].

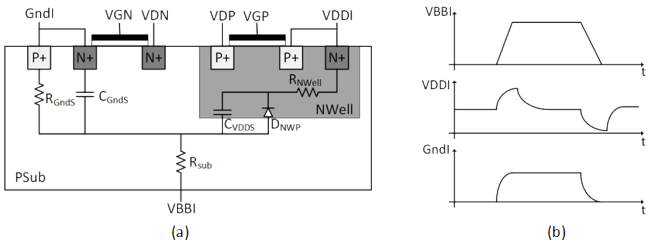

Fig. 13: (a) BBI effects on CMOS logic (cross sectional view), and (b) forward BBI effects on V_{DD} and ground nodes [43].

mixed-signal IC consisting of digital logic along with a phase-locked-loop [44]. Voltage glitches can have devastating effects in frequency synthesis and can induce large variations in the output voltage of bandgap references. These voltage glitches can be produced using body biasing attacks [43]. The body biasing injection (BBI) method applies high voltage pulses on the circuit substrate, thereby modifying the capacitive and/or resistive coupling between the substrate and power supply or ground, as shown in Figure 13(a). This, in turn, locally affects the power supply and/or ground voltages, as depicted in Figure 13(b), and can practically result in large deviations of power supply voltage values, as has been experimentally demonstrated in [43]. However, this requires that the packaged IC needs to be opened, in order to apply a very high and short substrate bias pulse.

III. AMS/RF IC/IP Piracy and Counterfeiting

As the complexity of electronic systems has significantly increased over the past years, the market of reusable IPs has tremendously grown. As a result, the vast majority of silicon dice and systems-on-chips currently comprise AMS IP blocks which are produced by third party companies. Unlike their digital counterparts, whose security concerns have been addressed during the last two decades, solutions for protecting AMS/RF IPs against reverse engineering and theft have only recently been proposed. The same holds for AMS/RF IP counterfeiting, which is considered a problem growing in magnitude [45], [46].

IP piracy scenarios can be staged either in the foundry level, e.g. through reverse engineering and illegal copying of an IP, or after the IP has been produced, e.g. claiming ownership and reselling it as a black box [47]. Reverse engineering can be performed at the chip-, printed circuit board- and system-level [48]. Many practical examples of counterfeit ICs with an increased level of sophistication, typically deployed after the IC has been produced, have also been reported raising health and safety concerns [45], [46]. To prevent reverse engineering, obfuscation-based techniques applied either at the netlist or at the layout level (camouflaging) have been used to transform a design into one that is functionally equivalent to the original but much more difficult to reverse engineer [48], [49]. Along with obfuscation, logic encryption was recently introduced to encrypt the functionality of a design and protect it from malicious insertions by untrusted foundries [8], [50]. IC ownership and authenticity can be preserved via watermarking [47], which uniquely encodes the signature of the author both in the netlist and the physical implementation stages. Finally, several counterfeit detection methods have been proposed, which can be classified into physical and electrical inspections, and aging-based fingerprints [45], [51]. More details on the above-mentioned existing detection and prevention methods against reverse engineering and counterfeiting are provided in [8], [45]–[50]. Despite the extensive effort in the digital domain, in the AMS/RF domain only a small number of defenses against piracy and counterfeiting have been reported.

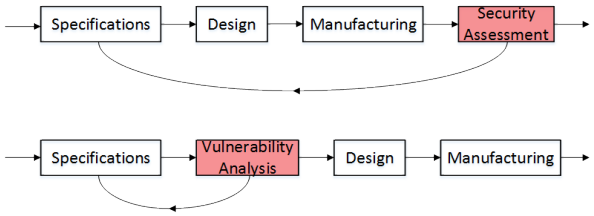

Fig. 14: AMS IP design flow before and after vulnerability analysis [52].

Accordingly, existing remedies for AMS/RF piracy and counterfeiting are described below:

A. Vulnerability Analysis

In [52], the authors propose an analysis in order to expose all vulnerabilities existent in the design of an analog IP. The methodology aims to identify potential security breaches in analog IP blocks and has to be performed after the IP specifications stage rather than after manufacturing, as shown in Figure 14. The IP block used for demonstrating the method is an analog block generating a clock signal, which consists of a bandgap reference, a voltage doubler, and a voltage controlled oscillator. The sub-functions of each of the sub-circuits are analyzed and the faults, as well as their signatures, are identified. Finally, the potential attacks for each of the faults are evaluated, along with the identifying potential, which expresses the time and effort required for an adversary to identify the attack. Once all attacks have been identified, appropriate countermeasures can be taken by the designer.

B. Split Manufacturing

Split manufacturing was recently proposed to protect analog/RF IPs from reverse engineering at the foundry level [53]. The key idea of split manufacturing is to protect designs by dividing manufacturing chips into front end of line (FEOL) and back end of line (BEOL). Accordingly, FEOL and BEOL layers are fabricated in untrusted and trusted foundries, respectively. The general concept of this method was presented in a PA design for RF applications. Specifically, the top two metal layers of the technology were removed from the FEOL. In such a case, the inductors and capacitors of the PA become invisible to the attacker. The authors show that even if the inductor and capacitor positions and sizes can be estimated through the blank areas that are created, it is difficult to reverse engineer the chip given the wide range of component values, bias voltages and operating frequencies. In RF designs, inductors are placed in metal rings and lower metal layers inside the rings are removed for performance optimization. Therefore, the rings themselves may indicate the exact position and size of the inductors. To counteract this issue, the authors obfuscate the original design by inserting non-functional rings and creating empty zones. The empty blocks in the layout increase performance overhead; however, this can be alleviated if the designers consider security in the early design stages.

C. AMS IP Watermarking

To protect AMS IP ownership, a layout watermarking method was proposed in [54], [55]. This method uses an algorithm to parse the layout netlist and sort transistors one level at a time, based on their type (NMOS or PMOS), width, shortest distance to input, and shortest distance to output. The outcome of the search algorithm, whose pseudocode is provided below, is a uniquely ordered list of transistors.

Algorithm 1 Pseudocode for ordering transistors [54]

```
Make a dummy transistor
Connect it to all of the inputs of the circuit
Add the dummy transistor to the FIFO queue
while queue is not empty do
   De-queue the next transistor
   if it is not marked visited then
      for the set of successor transistors do
         if any are matched then
            group them together
            rank by channel type, width and distance to output
         end if
         if any are indistinguishable then
            treat as matched
            add the ordered transistors to the FIFO queue
            append them to the final sequential array
         end if
      end for
      Mark the current transistor visited
   end if
end while
```

Once this list has been created, the owner generates the watermark he/she wants as a seed for a pseudo-random number generator. The bits which are generated from the random function form a long bitstream that can be aligned with the stream of uniquely sorted transistors. The bitstream is embedded by fingering the transistors depending on the bit that aligns with each transistor. A bit value of "1" or "0" corresponds to an even or odd number of fingers, respectively. Using this method a design entity A, having a netlist A can prove ownership of an IP against a design entity B, having a netlist B. The IP owner can look into the nodes of the ordered array of netlist B and generate bitstream B, corresponding to the odd or even number of transistor fingers. The owner who has two bitstreams, A and B, can measure the degree of correlation between them. Unless the design entity B generates the correct seed for bitstream B, the design entity A can claim that B has stolen the layout. This technique has been effectively applied to a two-stage Miller operational amplifier. The watermarked layout suffered only 0.25% increase in the chip area.

D. AMS Counterfeit Protection

Analog ICs are among the 5 most counterfeited parts [56]. However, only a few protection mechanisms against counterfeiting have been reported. In [57], protection against recycled analog ICs was achieved using statistical methods, such as one-class classifiers and degradation curve sensitivity analysis. Typical test results from production early failure rate analysis, such as minimum supply voltage (V_{min}), quiescent current (I_{ddq}), and maximum oscillation frequency (F_{max}) were

used as parametric measurements for evaluating both methods. Results were demonstrated in a fully differential folded cascode operational amplifier designed in a 45nm technology node, showing that both methods were able to achieve 100% correct classification between brand new and recycled devices. Recently, low-cost, on-chip ring oscillators were used for protecting ICs against recycling [58]. It is likely that such an approach can be also applicable in AMS/RF ICs.

IV. Limitations of Existing Work

After over a decade of intense research efforts by numerous groups around the world, the objective of ensuring trustworthiness of digital ICs is a fairly well-understood and quite mature topic. Indeed, a large number of alternative threat scenarios, as well as detection and/or prevention methods, have been experimentally evaluated, often using actual silicon measurements. On the other hand, the operational complexity and the continuous-domain characteristics of AMS/RF ICs, have served as challenges which have limited the community's collective understanding, modeling and mitigating of security risks in the AMS/RF domain. Among the most notable contributions in this domain, we pinpoint the effectiveness of hardware Trojans in modifying the RF front-end of cryptographic ICs to steal sensitive information, which has been experimentally demonstrated in silicon. In the AMS world, the key contribution to date is the demonstration of innate Trojan states, which may potentially result in undesired operating conditions. A few concepts of analog triggers, which have mostly been used to compromise digital circuits, and a few protection mechanisms against analog IP theft and reverse engineering complete the picture of the rather limited literature on this subject matter. Moving forward, a number of limitations in existing studies need to be addressed in order to raise our understanding of the problem to the next level and lead to breakthroughs in this area. For example:

- In AMS circuits, security implications have only been shown in a few basic analog blocks; moreover, all of the relevant work is based on simulations. While simulations are informative, demonstration and evaluation through actual silicon implementation is needed for drawing definitive conclusions.
- How an AMS circuit can be triggered to enter an undesired state and what the payload of such a Trojan state might be, other than circuit malfunction or denial of service, should be further investigated and better understood. Most of the current incarnations are either too simplistic or too unrealistic to be considered a real threat.
- Trojan-agnostic, systematic and generalizable detection/prevention methods need to be developed for AMS/RF ICs, rather than the current ad-hoc solutions. While this is inherently difficult in the analog domain, it is nevertheless important in order to facilitate automation and development of pertinent metrics.
- Formal methods for protecting AMS/RF ICs are still at their infancy and are urgently required. While analog formal verification has made great strides recently, its findings have yet to be applied in the security domain.

V. Conclusion

Despite the objective difficulties imposed by the continuous domain, the research community has realized that the security and trustworthiness risk is increased by AMS/RF ICs which may be the weakest link of an electronic system. Accordingly, there is a surge of activity in this area, seeking to develop security and trust solutions for AMS/RF ICs and IPs. Nevertheless, an extensive research effort, spearheaded by governmental and/or industrial support akin to that enjoyed by the digital domain over the last decade, has yet to materialize and is urgently needed in order for security and trustworthiness solutions for AMS/RF ICs and IPs to become up to par with their digital counterparts.

References

[1] S. Adee, "The Hunt For The Kill Switch," *IEEE Spectrum*, vol. 45, no. 5, pp. 34–39, May 2008.

[2] "Could a vulnerable computer chip allow hackers to down a Boeing 787. Back door could allow cyber-criminals a way in," https://goo.gl/i7aqm5, 2012.

[3] "F.B.I. says the military had bogus computer gear," https://goo.gl/QT90Nx, 2008.

[4] "Fishy Chips: Spies Want to Hack-Proof Circuits," https://goo.gl/wmJ2yL, 2011.

[5] J. Markoff, "Dell warns of hardware Trojan," https://goo.gl/MQ8jYr, 2010.

[6] M. Tehranipoor and F. Koushanfar, "A Survey of Hardware Trojan Taxonomy and Detection," *IEEE Design Test of Computers*, vol. 27, no. 1, pp. 10–25, 2010.

[7] 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.

[8] M. Rostami, F. Koushanfar, and R. Karri, "A Primer on Hardware Security: Models, Methods, and Metrics," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1283–1295, 2014.

[9] 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.

[10] Y. Jin, D. Maliuk, and Y. Makris, "Hardware Trojan Detection in Analog/RF Integrated Circuits," in *Secure System Design and Trustable Computing*. Springer, 2016, pp. 241–268.

[11] I. Polian, "Security Aspects of Analog and Mixed-Signal Circuits," in *IEEE International Mixed-Signal Testing Workshop (IMSTW)*, 2016, pp. 1–6.

[12] K. S. Subrmani, A. Antonopoulos, A. A. Abotabl, A. Nosratinia, and Y. Makris, "INFECT: INconsicuous FEC-based Trojan: a Hardware Attack on an 802.11a/g Wireless Network," in *IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, 2017.

[13] 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 Systems*, vol. 25, no. 4, pp. 1506–1519, 2017.

[14] Y. Liu, Y. Jin, and Y. Makris, "Hardware Trojans in Wireless Cryptographic ICs: Silicon Demonstration & Detection Method Evaluation," in *International Conference on Computer-Aided Design (ICCAD)*, 2013, pp. 399–404.

[15] D. Chang, B. Bakkaloglu, and S. Ozev, "Enabling Unauthorized RF Transmission Below Noise Floor with no Detectable Impact on Primary Communication Performance," in *IEEE VLSI Test Symposium (VTS)*, 2015, pp. 1–4.

[16] L. Lin, W. Burleson, and C. Paar, "MOLES: Malicious Off-chip Leakage Enabled by Side-channels," in *IEEE International Conference on Computer-Aided Design (ICCAD)*, 2009, pp. 117–122.

[17] R. O. Nielsen and A. N. Willson, "A Fundamental Result Concerning the Topology of Transistor Circuits with Multiple Equilibria," *Proceedings of the IEEE*, vol. 68, no. 2, pp. 196–208, 1980.

[18] R. M. Fox and M. Nagarajan, "Multiple Operating Points in a CMOS Log-domain Filter," in *IEEE International Symposium on Circuits and Systems (ISCAS)*, 1999, pp. 689–692.

[19] X. Cao, Q. Wang, R. L. Geiger, and D. J. Chen, "A Hardware Trojan Embedded in the Inverse Widlar Reference Generator," in *IEEE International Midwest Symposium on Circuits and Systems (MWSCAS)*, 2015, pp. 1–4.

[20] Q. Wang, R. L. Geiger, and D. J. Chen, "Challenges and Opportunities for Determining Presence of Multiple Equilibrium Points with Circuit Simulators," in *IEEE International Midwest Symposium on Circuits and Systems (MWSCAS)*, 2014, pp. 406–409.

[21] Q. Wang and R. L. Geiger, "Temperature Signatures for Performance Assessment of Circuits with Undesired Equilibrium States," *Electronics Letters*, vol. 51, no. 22, pp. 1756–1758, 2015.

[22] Q. Wang, R. L. Geiger, and D. Chen, "Hardware Trojans Embedded in the Dynamic Operation of Analog and Mixed-Signal Circuits," in *National Aerospace and Electronics Conference (NAECON)*, 2015, pp. 155–158.

[23] 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 *IEEE International Symposium on Circuits and Systems (ISCAS)*, 2014, pp. 289–292.

[24] Y. T. Wang, D. J. Chen, and R. L. Geiger, "Effectiveness of Circuit-level Continuation Methods for Trojan State Elimination Verification," in *IEEE International Midwest Symposium on Circuits and Systems (MWSCAS)*, 2013, pp. 1043–1046.

[25] C. Cai and D. Chen, "Performance Enhancement Induced Trojan States in OP-AMPS, their Detection and Removal," in *IEEE International Symposium on Circuits and Systems (ISCAS)*, 2015, pp. 3020–3023.

[26] Y. T. Wang, D. J. Chen, and R. L. Geiger, "Effectiveness of Circuit-level Continuation Methods for Trojan State Elimination Verification," in *IEEE International Midwest Symposium on Circuits and Systems (MWSCAS)*, 2013, pp. 1043–1046.

[27] D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi, and B. Sunar, "Trojan Detection Using IC Fingerprinting," in *IEEE Symposium on Security and Privacy (SP)*, 2007, pp. 296–310.

[28] Y. Jin and Y. Makris, "Hardware Trojan Detection Using Path Delay Fingerprint," in *IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, 2008, pp. 51–57.

[29] Y. Liu, K. Huang, and Y. Makris, "Hardware Trojan Detection Through Golden Chip-Free Statistical Side-Channel Fingerprinting," in *IEEE Design Automation Conference (DAC)*, 2014, pp. 155:1–155:6.

[30] F. Karabacak, U. Y. Ogras, and S. Ozev, "Detection of Malicious Hardware Components in Mobile Platforms," in *International Symposium on Quality Electronic Design (ISQED)*, 2016, pp. 179–184.

[31] Y. Liu, G. Volanis, K. Huang, and Y. Makris, "Concurrent Hardware Trojan Detection in Wireless Cryptographic ICs," in *IEEE International Test Conference (ITC)*, 2015, pp. 1–8.

[32] M. Bidmeshki, A. Antonopoulos, and Y. Makris, "Information Flow Tracking in Analog/Mixed-Signal Designs through Proof-Carrying Hardware IP," in *IEEE Design Automation and Test in Europe Conference (DATE)*, 2017.

[33] S. Deyati, B. J. Muldrey, and A. Chatterjee, "Targeting Hardware Trojans in Mixed-Signal Circuits for Security," in *IEEE International Mixed-Signal Testing Workshop (IMSTW)*, 2016, pp. 1–4.

[34] J. Roychowdhury and R. Melville, "Delivering Global DC Convergence for Large Mixed-Signal Circuits via Homotopy/Continuation Methods," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 25, no. 1, pp. 66–78, 2006.

[35] Z. Liu, Y. Li, R. L. Geiger, and D. Chen, "Auto-identification of Positive Feedback Loops in Multi-state Vulnerable Circuits," in *IEEE VLSI Test Symposium (VTS)*, 2014, pp. 1–5.

[36] Y. T. Wang, D. Chen, and R. L. Geiger, "Practical Methods for Verifying Removal of Trojan Stable Operating Points," in *IEEE International Symposium on Circuits and Systems (ISCAS)*, 2013, pp. 2658–2661.

[37] Y. T. Wang, Q. Wang, D. Chen, and R. L. Geiger, "Hardware Trojan State Detection for Analog Circuits and Systems," in *IEEE National Aerospace and Electronics Conference*, 2014, pp. 364–367.

[38] W. Hou, "Use of a continuation method for analyzing start-up circuits," Ph.D. dissertation, UNIVERSITY OF CALIFORNIA, IRVINE, 2011.

[39] A. V. Karthik and J. Roychowdhury, "ABCD-L: Approximating Continuous Linear Systems Using Boolean Models," in *IEEE Design Automation Conference (DAC)*, 2013, pp. 1–9.

[40] A. V. Karthik, S. Ray, P. Nuzzo, A. Mishchenko, R. Brayton, and J. Roychowdhury, "ABCD-NL: Approximating Continuous Non-Linear Dynamical Systems Using Purely Boolean Models for Analog/Mixed-Signal Verification," in *IEEE Asia and South Pacific Design Automation Conference (ASP-DAC)*, 2014, pp. 250–255.

[41] M. H. Zaki, O. Hasan, S. Tahar, and G. Al-Sammane, "Framework for Formally Verifying Analog and Mixed-Signal Designs," in *Computational Intelligence in Analog and Mixed-Signal (AMS) and Radio-Frequency (RF) Circuit Design*. Springer International Publishing, 2015, pp. 115–145.

[42] K. Yang, M. Hicks, Q. Dong, T. Austin, and D. Sylvester, "A2: Analog Malicious Hardware," in *IEEE Symposium on Security and Privacy (SP)*, 2016, pp. 18–37.

[43] N. Beringuier-Boher, M. Lacruche, D. El-Baze, J.-M. Dutertre, J.-B. Rigaud, and P. Maurine, "Body Biasing Injection Attacks in Practice," in *Workshop on Cryptography and Security in Computing Systems*, 2016, pp. 49–54.

[44] N. Beringuier-Boher, K. Gomina, D. Hely, J. B. Rigaud, V. Beroulle, A. Tria, J. Damiens, P. Gendrier, and P. Candelier, "Voltage Glitch Attacks on Mixed-Signal Systems," in *Euromicro Conference on Digital System Design*, 2014, pp. 379–386.

[45] U. Guin, K. Huang, D. DiMase, J. M. Carulli, M. Tehranipoor, and Y. Makris, "Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1207–1228, 2014.

[46] U. Guin, D. DiMase, and M. Tehranipoor, "Counterfeit Integrated Circuits: Detection, Avoidance, and the Challenges Ahead," *Journal of Electronic Testing*, vol. 30, no. 1, pp. 9–23, 2014.

[47] M. M. Tehranipoor, U. Guin, and D. Forte, "Hardware IP Watermarking," in *Counterfeit Integrated Circuits: Detection and Avoidance*. Springer International Publishing, 2015, pp. 203–222.

[48] S. E. Quadir, J. Chen, D. Forte, N. Asadizanjani, S. Shahbazmohamadi, L. Wang, J. Chandy, and M. Tehranipoor, "A Survey on Chip to System Reverse Engineering," *ACM Journal on Emerging Technologies in Computing Systems*, vol. 13, no. 1, pp. 6:1–6:34, 2016.

[49] J. Rajendran, M. Sam, O. Sinanoglu, and R. Karri, "Security Analysis of Integrated Circuit Camouflaging," in *ACM Conference on Computer & Communications Security (CCS)*, 2013, pp. 709–720.

[50] J. Rajendran, H. Zhang, C. Zhang, G. S. Rose, Y. Pino, O. Sinanoglu, and R. Karri, "Fault Analysis-Based Logic Encryption," *IEEE Transactions on computers*, vol. 64, no. 2, pp. 410–424, 2015.

[51] K. Xiao, D. Forte, and M. Tehranipoor, "Circuit Timing Signature (CTS) for Detection of Counterfeit Integrated Circuits," in *Secure System Design and Trustable Computing*. Springer International Publishing, 2016, pp. 211–239.

[52] N. Beringuier-Boher, D. Hely, V. Beroulle, J. Damiens, and P. Candelier, "Increasing the Security Level of Analog IPs by Using a Dedicated Vulnerability Analysis Methodology," in *International Symposium on Quality Electronic Design (ISQED)*, 2013, pp. 531–537.

[53] Y. Bi, J. S. Yuan, and Y. Jin, "Beyond the Interconnections: Split Manufacturing in RF Designs," *Electronics*, vol. 4, no. 3, pp. 541–564, 2015.

[54] D. L. Irby, R. D. Newbould, J. D. Carothers, J. J. Rodriguez, and W. T. Holman, "Low Level Watermarking of VLSI Designs for Intellectual Property Protection," in *IEEE International ASIC/SOC Conference*, 2000, pp. 136–140.

[55] R. D. Newbould, D. L. Irby, J. D. Carothers, J. J. Rodriguez, and W. T. Holman, "Mixed Signal Design Watermarking for IP Protection," in *Southwest Symposium on Mixed-Signal Design*, 2001, pp. 110–115.

[56] "Top 5 Most Counterfeited Parts Represent a $169 Billion Potential Challenge for Global Semiconductor Market," https://goo.gl/Ku4u6B, 2012.

[57] K. Huang, Y. Liu, N. Korolija, J. M. Carulli, and Y. Makris, "Recycled IC Detection Based on Statistical Methods," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 34, no. 6, pp. 947–960, 2015.

[58] U. Guin, D. Forte, and M. Tehranipoor, "Design of Accurate Low-Cost On-Chip Structures for Protecting Integrated Circuits Against Recycling," *IEEE Transactions on Very Large Scale Integration Systems*, vol. 24, no. 4, pp. 1233–1246, 2016.