Trusted Analog/Mixed-Signal/RF ICs: A Survey and a Perspective

Angelos Antonopoulos, Christiana Kapatsori, and Yiorgos Makris
University of Texas at Dallas

Editor's note:
The trustworthiness of integrated circuits is now an essential technical and business challenge for the semiconductor industry. In the digital domain, there has been extensive activity in understanding and counteracting the threats of hardware Trojans, piracy and counterfeiting. However, this research area is largely nascent and understudied for analog/mixed-signal (AMS) and radio frequency (RF) circuits, which are widely used in contemporary systems. This survey summarizes the state-of-art for trusted hardware design in AMS/RF IC's, and highlights directions towards advancing the field.

—Steven Nowick, Columbia University

■ **Trustworthiness of integrated** circuits (ICs) and circuit intellectual properties (IPs) has become a target of intense scrutiny and is now considered of major significance for the security of electronic circuits and systems, especially when deployed in sensitive industrial sectors, such as military, infrastructure, health, automotive, and telecommunication applications. Indeed, owing to various financial factors, the contemporary semiconductor industry relies on a complex business model, wherein the vast majority of IP design and IC fabrication is performed by third-party design houses and foundries. The globalized and highly distributed nature of the third-party entities, however, brings along trustworthiness concerns, as it results in a semiconductor supply chain model which exhibits several vulnerable points during the design, fabrication, and even the deployment phase of an IC, as depicted in Figure 1. These vulnerabilities may, then, be exploited by a knowledgeable adversary, thereby introducing various trustworthiness and security threats to the semiconductor industry and the end IC users. In general, such threats can be classified in two main categories, namely, hardware Trojans [1]–[3], and IC/IP piracy and counterfeiting [4]–[6].

While extensive research efforts have been expended over the last decade in understanding the threat of hardware Trojans and IP/IC piracy and counterfeiting, as well as in developing prevention and detection solutions in digital circuits, the topic remains largely unexplored for their analog/mixed-signal (AMS) and radio frequency (RF) counterparts. Given the widespread use of analog functionality (i.e., physical interfaces, sensors, actuators, wireless communications, and so on) in most contemporary systems, there is an alarming lack of understanding and an urgent need for a comprehensive study of the threat and solution space in the AMS/RF domain.[1] To this end, this survey paper seeks to summarize and present the existing, albeit limited work on known vulnerabilities and proposed remedies for AMS/RF ICs and IPs, as well as to elucidate the steps required toward designing, fabricating, and deploying trusted AMS/RF circuits.

Digital Object Identifier 10.1109/MDAT.2017.2728366
Date of publication: 18 July 2017; date of current version: 14 November 2017.

[1] To our knowledge, the only related article available in the open literature is [44], which mainly focuses on threats and countermeasures in digital ICs and briefly discusses their relevance in the AMS domain.

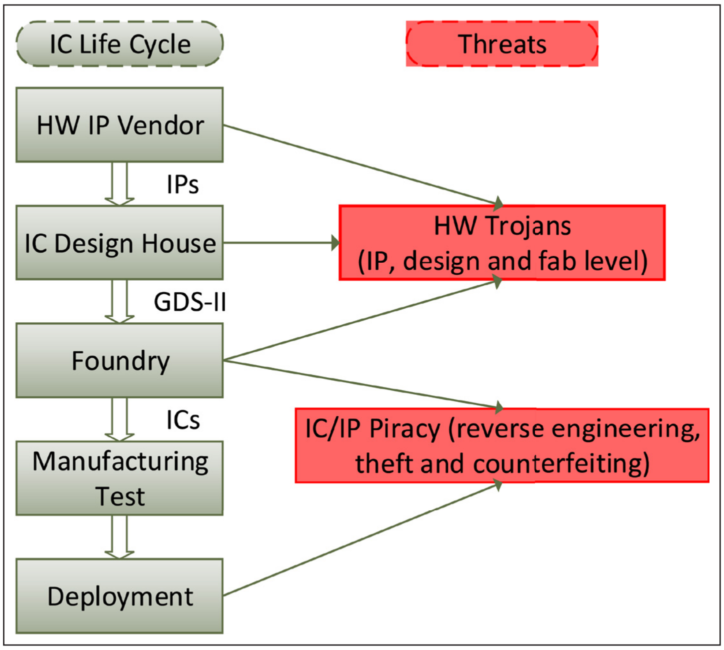
IC Life Cycle
Threats
HW IP Vendor
IPs
IC Design House
GDS-II
Foundry
ICs
Manufacturing Test
Deployment
HW Trojans (IP, design and fab level)
IC/IP Piracy (reverse engineering, theft and counterfeiting)

Figure 1. Threats in the IC and IP supply chain [1].

Security Risks in AMS/RF ICs

Recently, a few groups have demonstrated the possibility of covertly stealing sensitive information through hardware Trojans embedded in analog/RF ICs. In a different direction, multiple equilibrium states were shown to exist in basic blocks of AMS ICs, raising the concern that they could lead the circuit to an undesired (potentially malicious) state, unless appropriate remedies are taken. Hardware Trojan trigger mechanisms based on analog circuits, affecting the power supply of ICs and targeting mainly on digital microprocessors have also been reported. Finally, AMS/RF IP counterfeiting and reverse engineering is a concern growing in amplitude. The rest of this section elaborates on these four types of threats.

Hardware Trojans in RF ICs

Hardware Trojans can be introduced by untrusted IP vendors, by a rogue in-house element during the design (schematic and/or layout) stage of a product, or by an untrusted foundry directly at the fabrication mask level. In all cases, the hardware Trojan eventually becomes part of the actual functionality of the end product, unbeknownst to the legitimate designer and user. The risk that hardware Trojans pose intensifies in wireless networks where sensitive information is exchanged over public channels. This is the primary reason why existing hardware Trojan attacks have been targeting wireless ICs.

Hardware Trojans in wireless cryptographic ICs

An example of how minute modifications to a wireless cryptographic IC can leak the encryption key through a public channel was described and demonstrated through actual silicon measurements in [7] and [8]. The proposed hardware Trojans, one in the frequency and one in the amplitude domain, modify the ring oscillator or the power amplifier (PA) of an ultrawideband transmitter, adding a few extra transistors to modulate the leaked information on the amplitude or frequency characteristics of the transmitted signal, as shown in Figure 2a. Specifically, the transmission power waveform of each message bit exhibits slight but systematic increase of amplitude or frequency when the leaked key bit has value “0,” enabling differentiation from the case wherein the leaked key bit has value “1.” These minute modifications in the transmission power amplitude or frequency remain well within the margins allowed for dealing with semiconductor manufacturing process variation; accordingly, to the unsuspecting receiver, each transmission appears perfectly legitimate as it does not violate any of the circuit- or system-level specifications of the wireless cryptographic IC. To an informed adversary receiver, however, who is aware of the modulation implementation details and knows exactly what to look for in the transmission characteristics, retrieving the leaked encryption key is trivial. In this example, all the attackers have to do is observe the two distinct amplitude or frequency levels when the same message bit is transmitted and map them to a leaked key bit value of “0” or “1,” respectively.

To investigate the Trojan impact on the legitimate and rogue transmission, the authors in [8] implemented 15 distinct Trojan levels. 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 2b, where the measured transmission power for transmitting a ciphertext bit of “0” and “1” for 40 Trojan free, 40 amplitude-based Trojan-infested, and 40 frequency-based Trojan-infested ICs is plotted versus time. For the Trojan-infested transmissions, the maximum level of Trojan impact is employed. Each of the three distributions is enclosed in the μ+3σ envelop of the Trojan-free ICs [7], [8]. Interestingly, none of the Trojan-infested ICs falls out of the envelop boundaries.

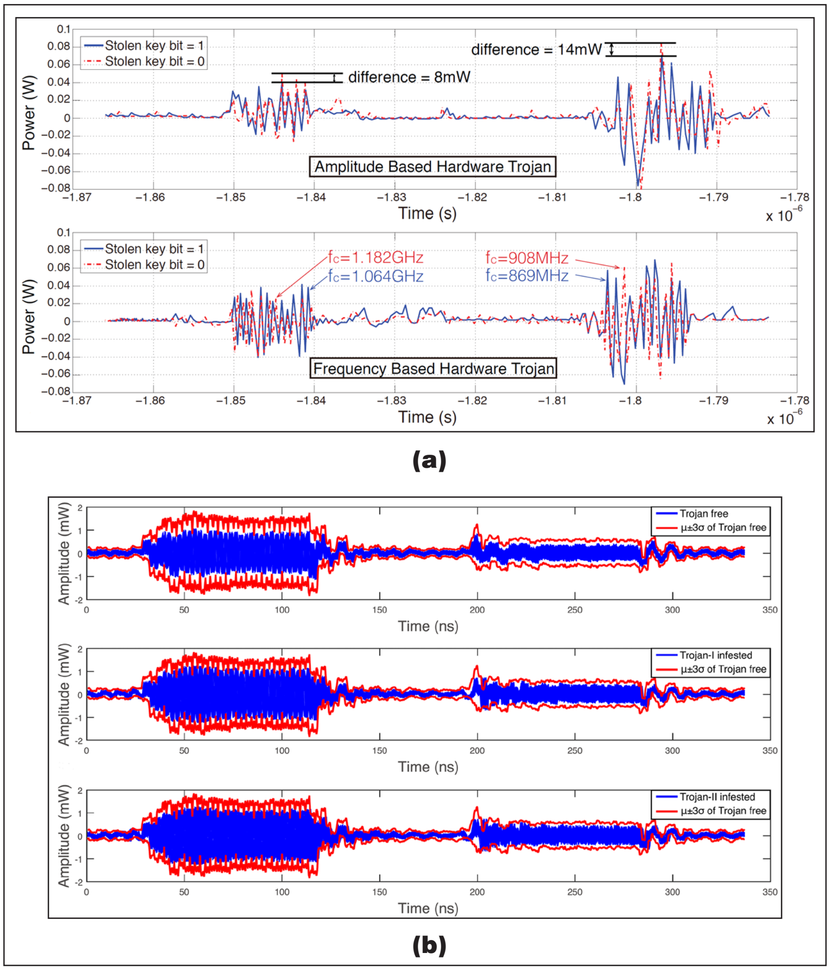

Figure 2. (a) Transmission power waveforms of amplitude- and frequency-based Trojan-infested ICs and (b) transmission power of 40 Trojan-free ICs, amplitude-based Trojan-infested ICs, and frequency-based Trojan-infested ICs enclosed in the μ+3σ transmission [7], [8].

RF transmission below noise floor

In a similar approach, the ability of hardware Trojans to hide unauthorized transmission signals in the ambient noise floor through spread spectrum techniques was presented in [9]. The original concept of communicating with attackers below the noise power level of a crypto-processor was initially demonstrated in [10], 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 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 [9] 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 3. The low-rate baseband data are 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. 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 multipath fading and multiple interferers. At the receiver, both the useful signal and interferers are mixed with the same spread-spectrum code, despreading 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 [9].

Hardware Trojans in AMS ICs

Unlike RF circuits, where a hardware Trojan adds extra circuitry to the legitimate structure to exploit its vulnerabilities, existing hardware Trojans in 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 inherently present in AMS components with feedback loops. This idea dates back to 1980, when it was shown that, for some choice of network parameter values, transistor

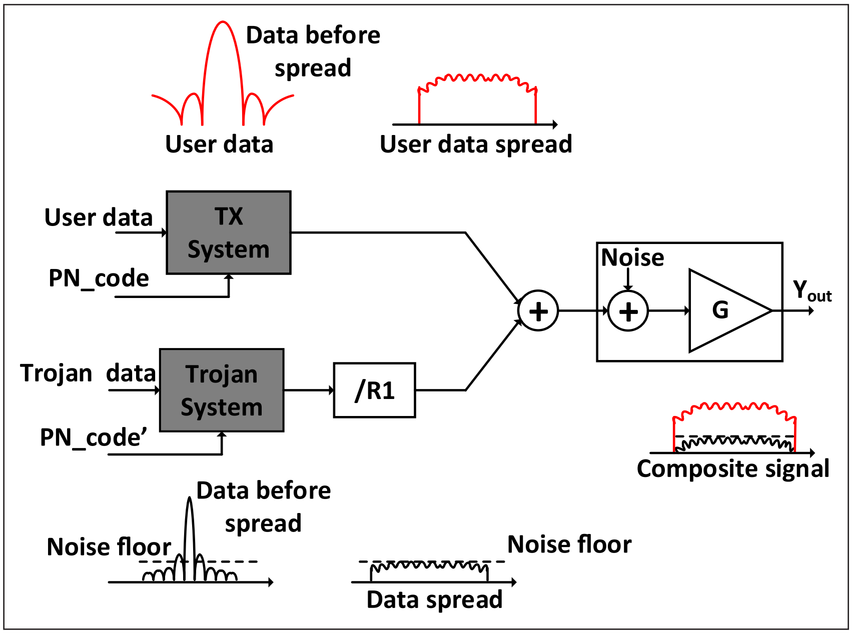

Figure 3. Spread spectrum technique used for evading detection of hardware Trojans in wireless networks [9].

networks with positive feedback loops can have more than one solution to their DC equations [11]. These multiple operating equilibrium points were demonstrated for verification purposes in a CMOS log-domain filter employing a positive feedback loop [12], 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 startup problem, meaning that a startup circuit should typically be added to remove the undesired state. However, if no startup circuit is used, which is quite common in analog design, or if the startup circuit is infiltrated, a redundant state harboring a Trojan may still exist [13].

Table 1. Circuit topologies in which Trojan states have been demonstrated via simulations.

Reference	Circuit Topology	Simulation Level
[12]	Log-domain filter	HSPICE
[13]	Inverse Widlar current mirror	Cadence Spectre
[14]	Op-amp	Cadence Spectre
[15]	Wien bridge oscillator	N/A
[16]	Bandgap reference	Cadence Spectre

In the last few years, 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/or 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, and Wien oscillators and filters [12]–[16]. These observations have been corroborated via simulations as indicated in Table 1. For example, due to the presence of multiple equilibrium points, while sweeping temperature in the Inverse Widlar mirror shown in Figure 4a, the output voltage may reach values other than the ones expected for a specific temperature [13]. Indeed, as plotted in Figure 4b more than one output voltage corresponds to temperatures T1 and T2, thus, indicating the existence of undesired, potentially malicious states. 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 [14]. Trojan states were also demonstrated via simulation results for the Wien bridge oscillator [15]. These states occur when high nonlinearities 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 [15]. 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.

Analog triggers

A key limitation of the AMS Trojan states discussed in the previous subsection stems from the lack of trigger mechanisms capable of driving a circuit into an undesired state. So far, only a few analog triggers have been presented in the literature.

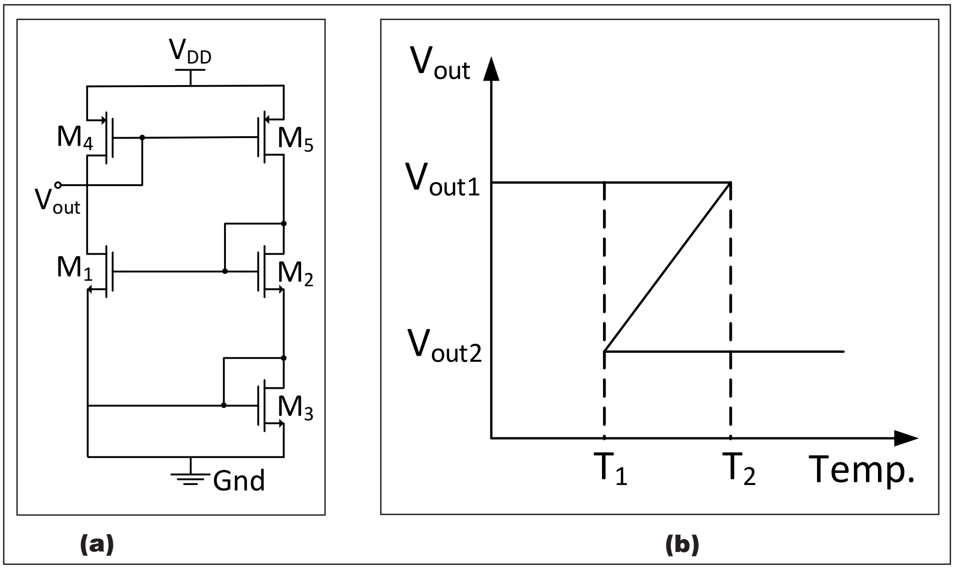

Figure 4. (a) Schematic of the Inverse Widlar current mirror and (b) multiple operating points in DC temperature sweep of the Inverse Widlar current mirror [13].

Capacitors

An analog trigger targeting a digital microprocessor was demonstrated in [17]. Similar to the principle first introduced in [10], wherein a capacitor of adjustable value is used to leak information conveyed by a power side-channel, the circuit in [17] employs capacitors to siphon charge from nearby (aggressor) wires as they undergo transition between digital values. When the capacitors fully charge, an attack to a victim flip-flop is staged [17]. In essence, the capacitor performs analog integration of charge from an aggressor wire while, at the same time, being able to reset itself through charge leakage. Every time the trigger input wire toggles, the capacitor's charge increases until its voltage exceeds a predetermined threshold, at which point the trigger output is activated. When the trigger input is inactive, the leakage current gradually reduces the capacitor's voltage and eventually deactivates the trigger output. A behavioral model of the operation of this analog trigger is depicted in Figure 5.

Voltage glitches

Voltage glitches of the power supply constitute another trigger mechanism whose impact has been shown on a mixed-signal IP consisting of digital logic along with a phased-locked-loop [18]. 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 [19]. The body biasing injection method applies high voltage pulses on the circuit substrate, thereby modifying the capacitive and/or resistive coupling between the substrate and the power supply or the ground, as shown in Figure 6a. This, in turn, locally affects the power supply and/or ground voltages, as depicted in Figure 6b, and can practically result in large deviations of power supply voltage values, as has been experimentally demonstrated in [19]. However, this requires that the packaged IC is opened, in order to apply a very high and short substrate bias pulse. The effect of voltage glitches in a bandgap reference was recently investigated in [18]. Specifically, it was shown that despite its inherent capability of providing a reference voltage with small variations with respect to changes in the supply voltage, excessive voltage glitches in the supply voltage were capable of driving transistors of the bandgap reference into their linear region, wherein bandgap functioning is not guaranteed.

AMS/RF Reverse Engineering and Counterfeiting

IP piracy has become a key concern due to the large volume of reusable IPs in silicon dice raising both safety and reliability concerns [4]. IP piracy scenarios, as shown in Figure 1, can be staged either at the foundry level, e.g., through reverse engineering and illegal copying of an IP, or after the IP has been produced, e.g., by claiming ownership and reselling it as a black box [5].

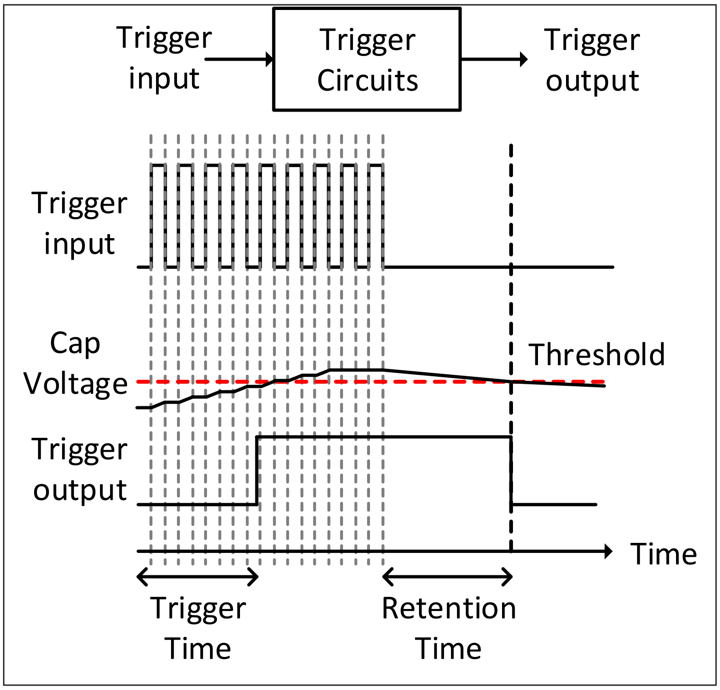

Figure 5. Behavioral model of the analog trigger circuit in [17].

Unlike past counterfeit practices, which relied on electronic waste to recycle, remark or repackage, and then sell old components as if they were new, modern clones are far more sophisticated [6]. The counterfeiters nowadays use advanced reverse engineering techniques to

- copy and reproduce the design of the original IC; and
- fabricate and package the IC from scratch.

Reverse engineering can be performed at the chip-, printed circuit board- or system-level. Among the various counterfeit electronic components, analog ICs are the most affected, corresponding to more than 25% of the reported counterfeit IC incidents in 2011 [4]. An example of a counterfeit IC, specifically an encoder, is shown in Figure 7. Evidently, by a simple inspection a buyer/user is incapable of distinguishing the original (bottom) from fake (top) components [6].

Countermeasures for AMS/RF ICs and IPs

Traditional test methods are ineffective in detecting hardware Trojans: 1) with small overhead (in terms of area and power); 2) which do not violate any protocol specifications; and 3) 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. Existing solutions against reverse engineering and counterfeiting in AMS/RF ICs are also discussed below.

Defenses against AMS/RF hardware Trojans

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 [20] and [21] 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 in the wireless cryptographic IC, which were presented previously. Production testing falls short in detecting such hardware Trojans, due to their negligible area and power overhead and the unaffected operation of the targeted chip. However, because of its systematic nature, the hardware Trojan imposes added statistical structure to the transmission characteristics and can be detected using statistical side-channel fingerprinting. This is depicted in Figure 8, where Trojan-free and Trojan-infested populations of the amplitude-based hardware Trojan are projected on three dimensions corresponding to the three principal components of the data after simple statistical processing using principal component analysis is applied. As may be observed, even a simple one-class classifier, such as a minimum volume enclosing ellipsoid, can be effectively trained to enclose the trusted population and can be subsequently used for distinguishing Trojan-free from Trojan-infested chips, as shown in Figure 8b. The same holds for the Trojan which operates in the frequency domain, and which can also be detected by the same statistical method. More details of this method which is Trojan-agnostic and can, therefore, detect any Trojan that systematically distorts transmission power in order to leak data, can be found in [8].

A method for detecting hardware Trojans operating below noise level, as well as hardware Trojans in mobile platforms, was presented in [22]. This method does not require a golden reference; rather, it is based on self-referencing. The output of a mobile platform running on a commercial MpSoC board is driven into a periodic steady state to decouple the response of the board from that of noise and Trojan. Any 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 of distinguishing 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 is detected.

Concurrent detection

Hardware Trojans which remain dormant at all times except during normal operation can easily evade detection by statistical side-channel fingerprinting methods since these methods operate either before an IC is deployed or, periodically, during idle times, after an IC is deployed. To counteract this issue, a concurrent hardware Trojan detection (CHTD) method which operates along with the normal functionality of the IC was presented in [23]. CHTD operates in real-time and does not require golden reference chips. 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. This method was capable of revealing malicious activity of the Trojans in wireless cryptographic ICs, which were previously described.

Homotopy methods

Defense mechanisms that have recently been applied for detecting multiple operating points in analog circuits with positive feedback loops are based on homotopy theory, which has been long used for verification purposes [24]. Given an analog circuit, the first step toward 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 and assigning signs for voltage/current dependencies. For example, in the threshold voltage reference circuit shown in Figure 9a, the dependency graph, depicted in Figure 9b, consists of two loops. The positive feedback loop contains an even number of "negative" dependencies, and in this case it is shown in Figure 9c. After the positive feedback loops of the circuit have been identified, the continuation method can be applied to detect its undesired states. This 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

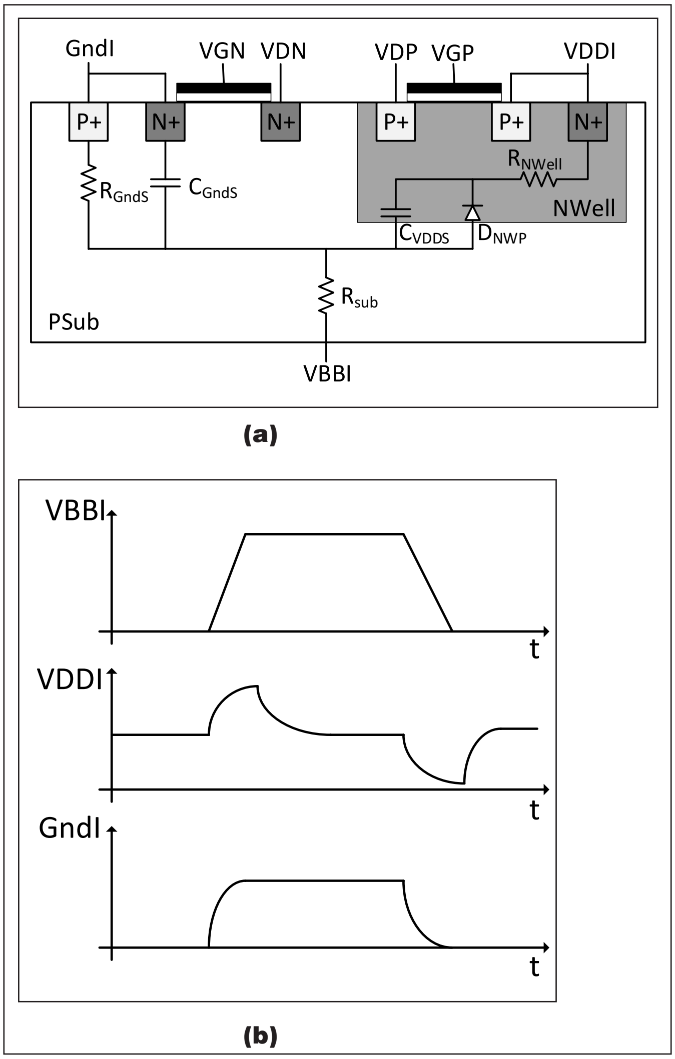

Figure 6. (a) Body biasing injection (BBI) effects on CMOS logic (cross sectional view) and (b) forward BBI effects on VDD and ground nodes [19].

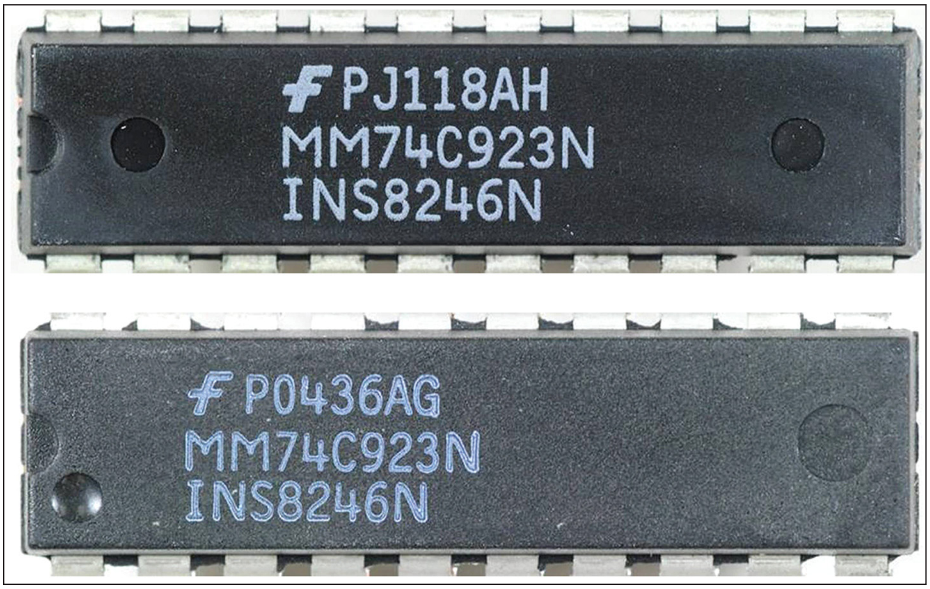

Figure 7. Fake (top) and original (bottom) encoder from Fairchild Semiconductor (now On Semiconductor) [6].

can be viewed as a homotopy approach applied to each positive feedback loop [25]. The continuation method has been demonstrated in several AMS ICs employing positive feedback loops [16], [26]–[28].

Formal methods

Another route toward detection of Trojan states in AMS circuits could be the use of formal verification methods for AMS designs after they have been approximated as purely Boolean models, as in [29]–[31]. However, this has not been investigated so far. The same holds for [32], 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. Recently, information flow tracking in AMS designs through proof-carrying hardware was shown in [33]. Specifically, integration of information flow tracking across the analog and digital domain allowed detection of sensitive data leakage from the analog to the digital domain, and vice versa, without requiring any modification of the AMS circuit design flow. This method could also be applied for verifying security properties, e.g., detection of multiple equilibrium points in AMS designs.

Parasitic loads and ad-hoc methods

Detection of hardware Trojans based on the signature left due to “rogue” load capacitances was also recently discussed for RF circuits in [34]. Specifically, stimulus optimization experiments were performed in a typical cascode low noise amplifier, enabling detection of small capacitive loads in several internal nodes, caused by the presence of hardware Trojans.

Ad-hoc methods for preventing undesired states in analog ICs can also be found in literature. Specifically, in [13], simulation results indicate that by decreasing the width of the diode-connected transistor M3 in the Inverse Widlar current mirror of Figure 4a, the region in which output voltages overlap and can, thus, result in Trojan states, can be eliminated. Finally, toward preventing unstable operating points, a startup circuit which forces the operating point to settle in a desired, stable state can be used, as described in [27].

Remedies against counterfeiting and reverse engineering

To prevent reverse engineering in digital ICs, obfuscation and logic encryption have been proposed [35], [36]. The former transforms a design into one that is functionally equivalent to the original one but much more difficult to reverse engineer, while the latter embeds the design in a larger functional space, requiring a key to unlock its functionality. In a different direction, IC ownership and authenticity can be preserved via watermarking [5], which uniquely encodes the signature of the author. Several counterfeit detection methods have been proposed, generally classified into electrical inspections, and aging-based fingerprints [4]. Finally, advanced imaging techniques can be employed to reveal the inner layers of microchips and PCBs. These are provided by companies such as TechInsights [6]. More details on the state-of-the-art in detection and prevention methods against reverse engineering and counterfeiting can be found in [4]–[6]. Unlike the extensive effort in the digital domain, only a small number of defenses against piracy and counterfeiting have been reported for AMS/RF ICs. This is mainly due to the high sensitivity of analog/RF nodes to parasitics.

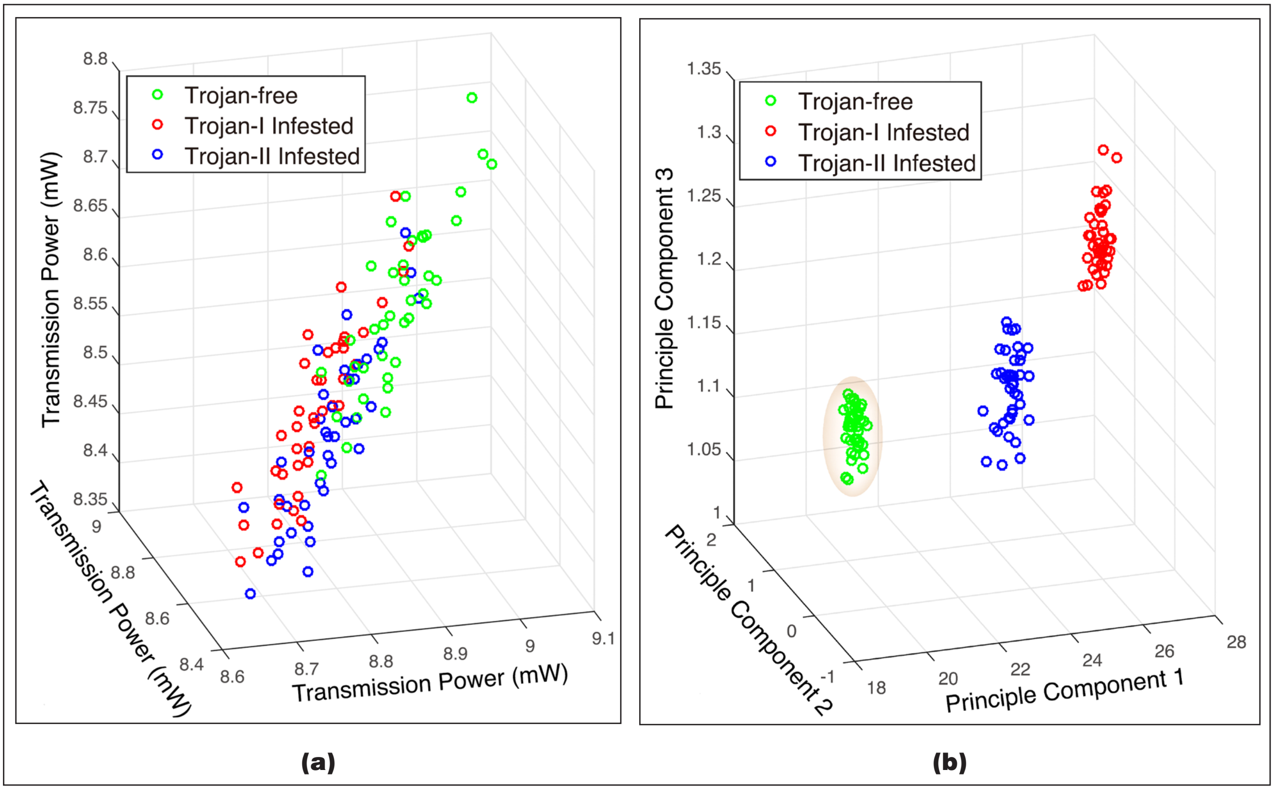

Figure 8. Trojan-free and Trojan-infested circuits projected on a 3D space where the populations are (a) indistinguishable and (b) distinguishable after applying principal component analysis [8].

This sensitivity makes obfuscation a hard task for analog/RF designers, since any extra transistor would create a tradeoff between obfuscation effectiveness and circuit performance. The few notable remedies for AMS/RF piracy and counterfeiting which can be found in the literature are summarized below.

Vulnerability analysis

In [37], the authors introduce an analysis methodology for exposing vulnerabilities which may exist in the design of an analog IP. More specifically, this methodology aims to identify potential security breaches in analog IP blocks and has to be performed after the IP specification stage rather than after manufacturing. The IP used for demonstrating this method is an analog block which generates a clock signal, consisting of a bandgap reference, a voltage doubler, and a voltage controlled oscillator. The subfunctions of each of the subcircuits are analyzed and the vulnerabilities (termed "faults" in this work) are identified along with their signatures. Finally, possible attacks which can take advantage of the presence of such faults are evaluated, along with the likelihood of being detected (termed "identifying potential"), expressed as the time and effort necessary for identifying an attack. Once all IP vulnerabilities have been identified, appropriate countermeasures can be recommended and applied by the designer in order to eliminate them.

Split manufacturing

Split manufacturing was recently proposed to protect analog/RF IPs from reverse engineering at the foundry [38]. The key idea of split manufacturing is to hide design details by dividing them into front end of line (FEOL) and back end of line (BEOL). Subsequently, 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. 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

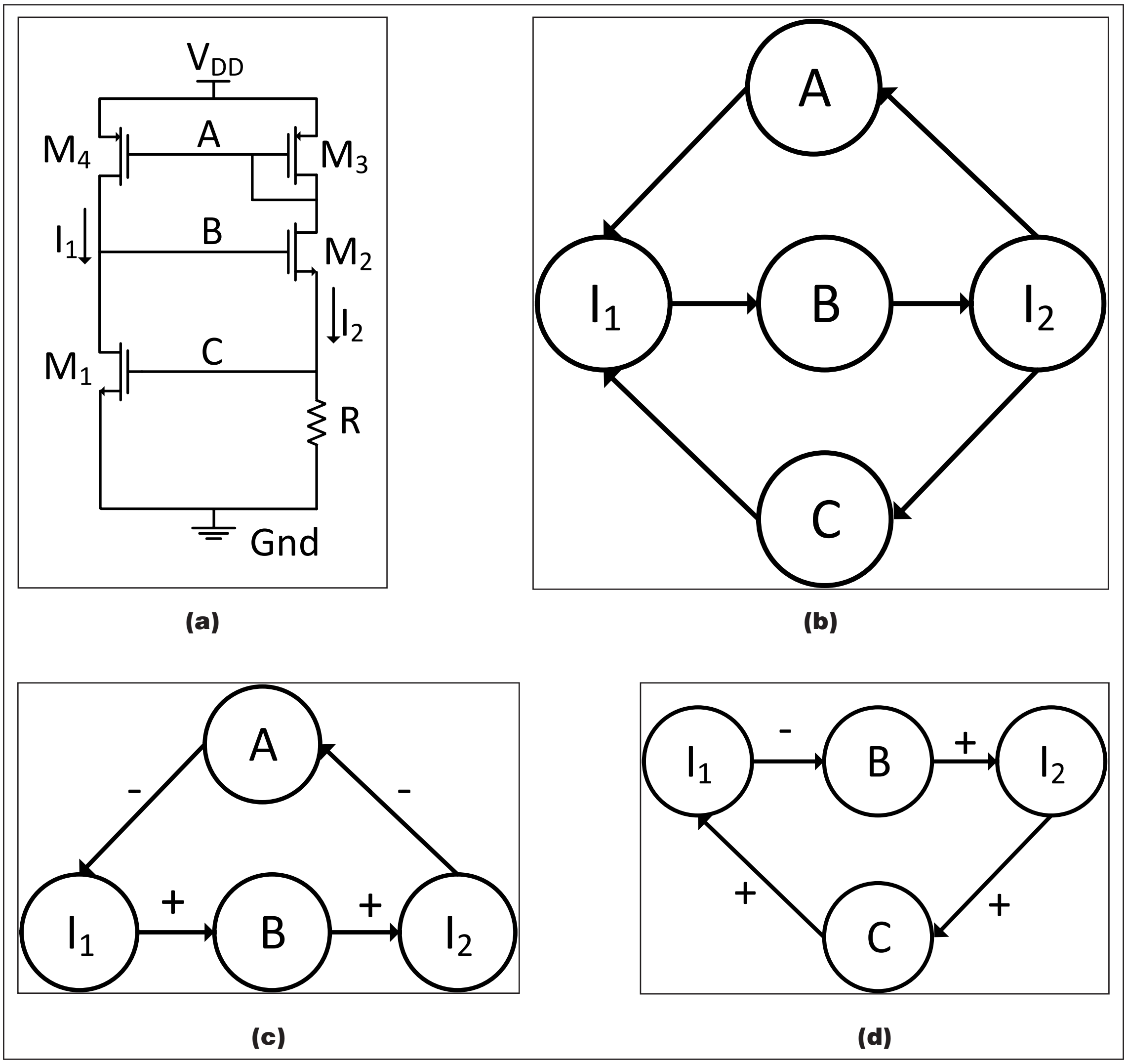

Figure 9. Bootstrapped threshold voltage reference circuit: (a) schematic, (b) directed dependency graphs, (c) dependence sign for the top loop, and (d) dependence sign for the bottom loop [16].

the inductors' and capacitors' 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 possible 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, the authors obfuscate the original design by inserting nonfunctional rings and creating empty zones. The empty blocks in the layout increase performance overhead, yet this can be alleviated if the designers consider security in the early design stages.

AMS IP watermarking

To protect AMS IP ownership, a layout watermarking method was proposed in [39]. 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 is a uniquely ordered list of transistors. Once this list has been created, the owner generates the watermark he/she wants as a seed for a pseudorandom number generator. The bits which are generated from the pseudorandom 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 which has the two bitstreams, A and B, can measure the degree of correlation between them. Unless design entity B generates the correct seed for bitstream B, design entity A can claim that design entity B has stolen the layout. This technique has been effectively applied to a two-stage Miller operational amplifier, where the watermarked layout suffered only a 0.25% increase in chip area.

Statistical/aging methods and on-chip sensors

In [4] and [40], 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. The results were demonstrated in a fully differential folded cascode operational amplifier designed in a 45-nm 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 and other aging sensors were used for protecting digital ICs against recycling [41]. While not explicitly reported in the literature yet, it is highly likely that such methods can also be adapted and can be applicable and effective in AMS and RF ICs as well.

Physical unclonable functions

An emerging solution for IC cloning is represented by physical unclonable functions (PUFs). PUFs have been lately adopted by major microelectronic companies such as Xilinx and Microsemi, for chip authentication [6]. A PUF is a function mapping challenges to responses, which is easy to evaluate but hard to characterize and reproduce [42]. Its unclonability stems from the fact that the function depends on a complex way upon several physical quantities that cannot be controlled by the manufacturing process [42]. PUFs rely on the physical variations among transistors, e.g., mismatch of MOSFET threshold voltages and statistical delay variation of circuits and interconnects in order to identify individual ICs. A PUF which uses dynamic latched comparators and their random input offset voltages (due to mismatches and noise) to create a unique response and protect an AMS design from counterfeiting was recently presented in [43]. Operation of this PUF was verified via experimental measurements using a 130-nm CMOS technology on two comparator types, i.e., double-tail and three-latch extended range comparators. Since comparators are an inherent component in many AMS designs, the implemented PUF can reuse comparators which are present in the design, thus, reducing its area overhead.

Discussion

After over a decade of intense research efforts by numerous groups around the world, the objective of ensuring trustworthiness of digital ICs and IPs 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 demonstrated and 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 analog/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 in order to covertly steal sensitive information, which has been experimentally demonstrated in silicon. In the AMS world, the key contribution to date consists in 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, several 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. Some of the examples are as follows:

- 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 are 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.
- Systematic, generalizable hardware Trojan 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, provably secure methods for protecting AMS/RF IPs 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 and trust domain.
- Finally, stronger collaboration between the research and industry community is required so that technology and knowledge can be efficiently transferred both ways, toward achieving the common objective of trusted and reliable AMS/RF ICs.

To conclude, despite the objective difficulties imposed by the continuous domain, the research community has realized the important role of AMS/RF ICs in contemporary electronics, along with the security and trustworthiness risk they may incur as the weakest link of an electronic system. Accordingly, there appears to be a surge of activity in this area, with numerous new researchers seeking to contribute 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. Bhunia, M. S. Hsiao, M. Banga, and S. Narasimhan, “Hardware Trojan attacks: Threat analysis and countermeasures,” *Proc. IEEE*, vol. 102, no. 8, pp. 1229–1247, 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 Trans. Des. Autom. Electron. Syst.*, vol. 22, no. 1, pp. 6:1–6:23, May 2016.

[3] M. Rostami, F. Koushanfar, and R. Karri, “A primer on hardware security: Models, methods, and metrics,” *Proc. IEEE*, vol. 102, no. 8, pp. 1283–1295, 2014.

[4] 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,” *Proc. IEEE*, vol. 102, no. 8, pp. 1207–1228, 2014.

[5] M. Tehranipoor, U. Guin, and D. Forte, “Hardware IP watermarking,” in *Counterfeit Integrated Circuits: Detection and Avoidance.* Cham, Switzerland: Springer International, 2015, pp. 203–222.

[6] M. M. Tehranipoor, U. Guin, and S. Bhunia, “Invasion of the hardware snatchers,” *IEEE Spectr.*, vol. 54, no. 5, pp. 36–41, 2017.

[7] Y. Liu, Y. Jin, and Y. Makris, “Hardware Trojans in wireless cryptographic ICs: Silicon demonstration & detection method evaluation,” in *Int. Conf. Computer-Aided Design*, 2013, pp. 399–404.

[8] Y. Liu, Y. Jin, A. Nosratinia, and Y. Makris, “Silicon demonstration of hardware Trojan design and detection in wireless cryptographic ICs,” *IEEE Trans. Very Large Scale Integr. Syst.*, vol. 25, no. 4, pp. 1506–1519, 2017.

[9] D. Chang, B. Bakkaloglu, and S. Ozev, “Enabling unauthorized RF transmission below noise floor with no detectable impact on primary communication performance,” in *Proc. IEEE VLSI Test Symp.*, 2015, pp. 1–4.

[10] L. Lin, W. Burleson, and C. Paar, “MOLES: Malicious off-chip leakage enabled by side-channels,” in *Proc. Int. Conf. Computer-Aided Design*, 2009, pp. 117–122.

[11] R. O. Nielsen and A. N. Willson, “A fundamental result concerning the topology of transistor circuits with multiple equilibria,” *Proc. IEEE*, vol. 68, no. 2, pp. 196–208, Feb. 1980.

[12] R. M. Fox and M. Nagarajan, “Multiple operating points in a CMOS log-domain filter,” *IEEE Trans. Circuits Syst. II, Analog Digit. Signal Process.*, vol. 46, no. 6, pp. 705–710, Jun. 1999.

[13] X. Cao, Q. Wang, R. L. Geiger, and D. J. Chen, "A hardware Trojan embedded in the Inverse Widlar reference generator," in *Proc. IEEE Int. Midwest Symp. Circuits Syst.*, 2015, pp. 1–4.

[14] C. Cai and D. Chen, "Performance enhancement induced Trojan states in op-amps, their detection and removal," in *Proc. IEEE Int. Symp. Circuits Syst.*, 2015, pp. 3020–3023.

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

[16] 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 Int. Symp. Circuits Syst.*, 2014, pp. 289–292.

[17] K. Yang, M. Hicks, Q. Dong, T. Austin, and D. Sylvester, "A2 : Analog malicious hardware," in *Proc. IEEE Symp. Secur. Privacy*, 2016, pp. 18–37.

[18] N. Beringuier-Boher et al., "Voltage glitch attacks on mixed-signal systems," in *Proc. Euromicro Conf. Digital Syst. Des.*, 2014, pp. 379–386.

[19] N. Beringuier-Boher, M. Lacruche, D. El-Baze, J.-M. Dutertre, J.-B. Rigaud, and P. Maurine, "Body biasing injection attacks in practice," in *Proc. 3rd Workshop Cryptography Secur. Comput. Syst.*, 2016, pp. 49–54.

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

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

[22] F. Karabacak, U. Y. Ogras, and S. Ozev, "Detection of malicious hardware components in mobile platforms," in *Proc. Int. Symp. Quality Electron. Design*, 2016, pp. 179–184.

[23] Y. Liu, G. Volanis, K. Huang, and Y. Makris, "Concurrent hardware Trojan detection in wireless cryptographic ICs," in *Proc. IEEE Int. Test Conf.*, 2015, pp. 1–8.

[24] J. Roychowdhury and R. Melville, "Delivering global DC convergence for large mixed-signal circuits via homotopy/continuation methods," *IEEE Trans. Comput. Des. Integr. Circuits Syst.*, vol. 25, no. 1, pp. 66–78, 2006.

[25] Y. T. Wang, Q. Wang, D. Chen, and R. L. Geiger, "Hardware Trojan state detection for analog circuits and systems," in *Proc. IEEE Nat. Aerospace Electronics Conf.*, 2014, pp. 364–367.

[26] Q. Wang, R. L. Geiger, and D. J. Chen, "Challenges and opportunities for determining presence of multiple equilibrium points with circuit simulators," in *Proc. IEEE Int. Midwest Symp. Circuits Syst.*, 2014, pp. 406–409.

[27] Y. T. Wang, D. J. Chen, and R. L. Geiger, "Effectiveness of circuit-level continuation methods for Trojan state elimination verification," in *Proc. IEEE Int. Midwest Symp. Circuits Syst.,* 2013, pp. 1043–1046.

[28] Y. T. Wang, D. Chen, and R. L. Geiger, "Practical methods for verifying removal of Trojan stable operating points," in *Proc. IEEE Int. Symp. Circuits Syst.,* 2013, pp. 2658–2661.

[29] A. V Karthik and J. Roychowdhury, "ABCD-L: Approximating continuous linear systems using Boolean models," in *ACM/EDAC/IEEE Des. Autom. Conf.*, 2013, pp. 1–9.

[30] 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 *Proc. Asia South Pacific Des. Autom. Conf.*, 2014, pp. 250–255.

[31] A. Karthik, *Accurate Booleanization of Continuous Dynamics for Analog/Mixed-Signal Design*, EECS Department, University of California, Berkeley, CA, USA, 2016.

[32] 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*, M. Fakhfakh, E. Tlelo-Cuautle, and P. Siarry, Eds. Cham, Switzerland: Springer International, 2015, pp. 115–145.

[33] M. Bidmeshki, A. Antonopoulos, and Y. Makris, "Information flow tracking in analog/mixed-signal designs through proof-carrying hardware IP," in *Proc. IEEE Des. Autom. Test Europe Conf.*, 2017, pp. 1703–1708.

[34] S. Deyati, B. J. Muldrey, and A. Chatterjee, "Targeting hardware Trojans in mixed-signal circuits for security," in *Proc. IEEE Int. Mixed-Signal Testing Workshop*, 2016, pp. 1–4.

[35] J. Rajendran, M. Sam, O. Sinanoglu, and R. Karri, "Security analysis of integrated circuit camouflaging," in *ACM SIGSAC Conf. Comput. Commun. Secur.,* 2013, pp. 709–720.

[36] J. Rajendran et al., "Fault analysis-based logic encryption," *IEEE Trans. Comput.*, vol. 64, no. 2, pp. 410–424, Feb. 2015.

[37] 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 *Proc. Int. Symp. Quality Electron. Des.*, 2013, pp. 531–537.

[38] Y. Bi, J. S. Yuan, and Y. Jin, "Beyond the interconnections: Split manufacturing in RF designs," *Electronics*, vol. 4, no. 3, p. 541, 2015.

[39] N. Narayan, R. D. Newbould, J. D. Carothers, J. J. Rodriguez, and W. T. Holman, "IP protection for VLSI designs via watermarking of routes," in *IEEE Int. ASIC/SOC Conf.*, 2001, pp. 406–410.

[40] K. Huang, Y. Liu, N. Korolija, J. M. Carulli, and Y. Makris, "Recycled IC detection based on statistical methods," *IEEE Trans. Comput. Des. Integr. Circuits Syst.*, vol. 34, no. 6, pp. 947–960, Jun. 2015.

[41] U. Guin, D. Forte, and M. Tehranipoor, "Design of accurate low-cost on-chip structures for protecting integrated circuits against recycling," *IEEE Trans. Very Large Scale Integr. Syst.*, vol. 24, no. 4, pp. 1233–1246, 2016.

[42] S. Stanzione, D. Puntin, and G. Iannaccone, "CMOS silicon physical unclonable functions based on intrinsic process variability," *IEEE J. Solid-State Circuits*, vol. 46, no. 6, pp. 1456–1463, 2011.

[43] T. Bryant, S. Chowdhury, D. Forte, M. Tehranipoor, and N. Maghari, "A stochastic all-digital weak physically unclonable function for analog/mixed-signal applications," in *Proc. IEEE Int. Symp. Hardware Oriented Secur. Trust*, 2017, pp. 167–172.

[44] I. Polian, "Security aspects of analog and mixed-signal circuits," in *Proc. IEEE Int. Mixed-Signal Testing Workshop*, 2016, pp. 1–6.

Angelos Antonopoulos is a Post-Doctoral Research Associate at the University of Texas at Dallas, Richardson, TX, USA. His research interests include the design of robust and trusted integrated circuits and systems. He has a PhD in electronic engineering from the Technical University of Crete, Chania, Greece. He is a Member of the IEEE.

Christiana Kapatsori is currently a PhD student in the Electrical and Computer Engineering Department, University of Texas at Dallas, Richardson, TX, USA. Her research interests include hardware security focusing on analog/RF ICs. She holds an MSc in microelectronics from the University of Athens, Greece. She is a Student Member of the IEEE.

Yiorgos Makris is a Professor of Electrical Engineering at The University of Texas at Dallas, Richardson, TX, USA. His research interests include applications of machine learning in test, reliability, and security of ICs, with a particular emphasis on the analog/RF domain. He has a PhD in computer engineering from the University of California San Diego, La Jolla, CA, USA. He is a Senior Member of the IEEE.

■ Direct questions and comments about this article to Antonopoulos Angelos, Department of Electrical and Computer Engineering, The University of Texas at Dallas, Richardson, TX, 75080, USA; e-mail: aanton@utdallas.edu.