J Hardw Syst Secur (2018) 2:15–32
https://doi.org/10.1007/s41635-017-0024-z

Challenges and Opportunities in Analog and Mixed Signal (AMS) Integrated Circuit (IC) Security

Md Mahbub Alam[1] · Sreeja Chowdhury[1] · Beomsoo Park[1] · David Munzer[1] · Nima Maghari[1] · Mark Tehranipoor[1] · Domenic Forte[1]

Received: 8 May 2017 / Accepted: 7 November 2017 / Published online: 27 November 2017

Abstract In the last decade and so, a large amount of research has been done to secure hardware. Security features such as physically unclonable function (PUF), hardware metering, and obfuscation have been developed to protect hardware from threats. Detection and avoidance techniques for IC counterfeiting and hardware Trojan have been introduced to protect the IC supply chain. Till now, research has focused on digital ICs, but analog and mixed signal (AMS) ICs which hold the highest share in the market have been neglected. The solutions developed in digital domain for digital ICs do not extend well to AMS ICs. Thus, a major portion of the IC market remains unsecured. In this paper, we described the challenges and limitations associated with AMS IC security research focusing on three major sections: AMS-enabled security, counterfeiting, and AMS hardware Trojans. We also express a vision for AMS security research.

✉ Md Mahbub Alam
mahbub.alam@ufl.edu

Sreeja Chowdhury
sreejachowdhury@ufl.edu

Beomsoo Park
beomsoo0927@ufl.edu

David Munzer
munda01@ufl.edu

Nima Maghari
maghari@ece.ufl.edu

Mark Tehranipoor
tehranipoor@ece.ufl.edu

Domenic Forte
dforte@ece.ufl.edu

[1] Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL 32603, USA

Keywords AMS counterfeit IC · Analog suitable PUF · Hardware metering · Chaotic cryptography · Analog hardware Trojan

1 Introduction

ICs are the basic building blocks of the modern systems and infrastructures responsible for communication, energy, finance, defense, and much more. In general, an IC goes through a process like the one shown in Fig. 1 that includes design, fabrication, assembly, distribution, usage in a system, and end of life. The different stages are now performed in many places around the globe in order to reduce the cost and to meet the time to market. Over the last decade or so, this globalization has resulted in a tremendous increase in vulnerabilities within the IC supply chain [1, 2].

The design phase of integrated circuits is vulnerable to intellectual property (IP) piracy and hardware Trojan attacks [3] where a rogue employee can steal IPs and tamper RTL code that leads to modified functionality and/or back doors to leak secret information. During fabrication, an untrusted foundry can potentially counterfeit ICs by overproducing outside the contract and can tamper by inserting malicious circuits (hardware Trojans). Assembly packages the die and does the final test before shipping to the market. It is possible for an untrusted assembly to counterfeit the ICs by supplying defective chips or changing the grade of the ICs. The supply chain can also be infiltrated with counterfeit chips by unauthorized distributors. Attackers can reverse engineer the chip during its lifetime to gather information about the design to clone or tamper it. Finally, chips may be reclaimed from a system during its lifetime and resold at the market as new.

Hardware Trojans are intentionally created anomalies in a chip/circuit which remain hidden and are not easily

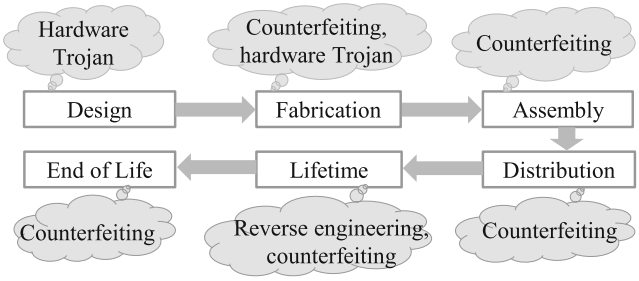

Fig. 1 IC supply chain vulnerabilities

detected or triggered [4, 5]. If a Trojan is triggered, it can change, degrade, or even stop the functionality of the circuit. While several solutions to counter hardware Trojans have been proposed by researchers, a majority of them pertain to digital ICs. Research related to hardware Trojans in analog and mixed signal (AMS) ICs has not yet developed much. Since AMS ICs have digital as well as analog components, Trojans in AMS chips can be digital, analog, or even mixed signal in nature [6]. The origin, effect, and countermeasures for these AMS Trojans can be fundamentally different from digital hardware Trojans which makes the existing approaches largely inapplicable.

Counterfeit parts that are used, defective, or generally nonconforming can severely impact the security and reliability of the critical electronic systems that unknowingly use them [1]. Particularly, counterfeit items in critical systems such as medical devices, transportation, or defense create life-threatening issues and lead to mission failure. It also creates a negative impact on corporate identity and revenue losses. The sale of counterfeits results in substantial economic losses to the electronics industry reportedly as high as $169 billion. Consequently, counterfeit detection and prevention have received considerable attention from researchers in recent years [1, 7]. While most of this work has been focused on digital ICs, analog ICs are in fact the most widely reported counterfeited parts among all types of popular semiconductors. Recent reports indicate that one out of every four counterfeit parts is an analog IC [8]. The increased complexity in supply chain and evolutionary nature of counterfeiters will make this problem even worse. Given the prevalence of analog counterfeits, it is imperative to develop counterfeit detection and prevention mechanisms for AMS ICs.

A large amount of research has focused on developing security features for large digital ICs such as physically unclonable functions (PUFs) [9], logic obfuscation [10], IC locking [11], and hardware metering to control the number of ICs. Security features require additional cost, area, and design complexity; thus, most of them are only applied to large digital ICs. Digitally designed features are not always realizable in AMS ICs and cannot be extended to AMS ICs directly. Analog and mixed signal-based security features may provide a solution to this issue and make AMS ICs more secure which holds a major portion of the IC market. Small digital ICs may also take advantage of analog security features.

The main barriers to establishing a secure supply chain for AMS ICs are lack of awareness, lack of systematic analysis of the security issues, and inapplicability of most digital solutions. In [12], some security aspects for AMS are discussed, but not in a comprehensive manner. For instance, countermeasures against reverse engineering, cloning, hardware Trojan, and side-channel attacks are discussed, but the challenges associated with implementing them are missing. In this work, we provide an analysis of AMS IC security that includes existing research in IC security, analyzes the applicability of prior works in AMS ICs, challenges in designing new IC security targeting AMS chips, and indicates the possible research directions for the community. We categorize our discussion into three major sections that can be summarized as follows:

i AMS-enabled security: We discuss the prospects of AMS security features concentrating on analog suitable PUFs and analog cryptomodules.
ii AMS IC counterfeiting: We examine the existing counterfeit detection and prevention techniques for AMS ICs and describe their limitations. We explore the potential solutions to overcome these limitations.
iii AMS hardware Trojan: Hardware Trojans affiliated with analog and mixed circuits are presented here. We classify the analog Trojans and describe the challenges with existing detection techniques.

The rest of the paper is organized as follows. In Section 3, we will discuss the challenges and opportunities in AMS-enabled security. The counterfeiting detection and avoidance techniques targeting AMS ICs are described in Section 4. Hardware Trojans in AMS signal circuit domains are discussed in Section 5. We conclude the paper in Section 6.

2 Preliminaries

In this section, we provide a comparison between AMS and digital ICs, and AMS IC classification in terms of integration and functionalities. This analysis will help us to understand the limitations, challenges, and opportunities associated with AMS IC security in later sections.

2.1 Digital IC vs. AMS IC

The major differences between analog and digital ICs are as follows:

- *Number of transistors and pins*: AMS chips have limited number of transistors and pins compared to digital ICs. Generally, the number of pins in AMS ICs is in the

range of less than 10 to 100 while digital ICs have 10 to several hundred pins.

- *Reverse engineering*: Reverse engineering requires a series of images be captured and stitched together [13]. Generally, AMS ICs are fabricated with older technology nodes, have a low count of transistors, and have lower circuit density, thereby making the imaging process much simpler.
- *Different verification procedures*: Test, verification, and characterization flows are fundamentally different in AMS chips compared to digital ones (more below).
- *Lack of cryptomodules*: Cryptomodules are typically designed in the digital domain [12].

2.2 AMS IC Types

AMS ICs are categorized based on the integration point of view into stand-alone and embedded ICs. Stand-alone AMS ICs are used singularly and are not a part of a microchip or system on chip (SoC). Alternatively, embedded AMS ICs in SoCs or microchip can be connected to multiple other components of the microchip which includes digital components. In this paper, both stand-alone and embedded ICs will be considered while discussing security features, counterfeit IC detection and prevention techniques, and hardware Trojans.

2.3 Design Flow of AMS and Digital ICs

A general design flow for analog and digital ICs from design specification to final IC product is depicted in Fig. 2. The design specifications are generally a set of functionalities that the final component will have to provide and a set of constraints such as power, size, and speed that it must satisfy. In analog ICs, the schematics are designed following the specifications and simulated using one of the several available circuit simulators at the transistor level. The key concept here is to design the circuits as close as possible to the required specification values. Next, physical designs are obtained by implementing layout of the design. The physical verification such as design rule check (DRC) and layout vs. schematic (LVS) are performed. A post-layout simulation measures the correctness of the design and implementation details. The chip is fabricated using a specific technology that has been specified at circuit design level. The process is completed by testing the IC with a number of test structures/vectors.

In digital ICs, high-level function descriptions and hardware description languages (HDL) are formed following the specifications. A behavioral simulation often at gate level ensures the correctness of the hardware design. The gate-level circuits are obtained through the synthesis,

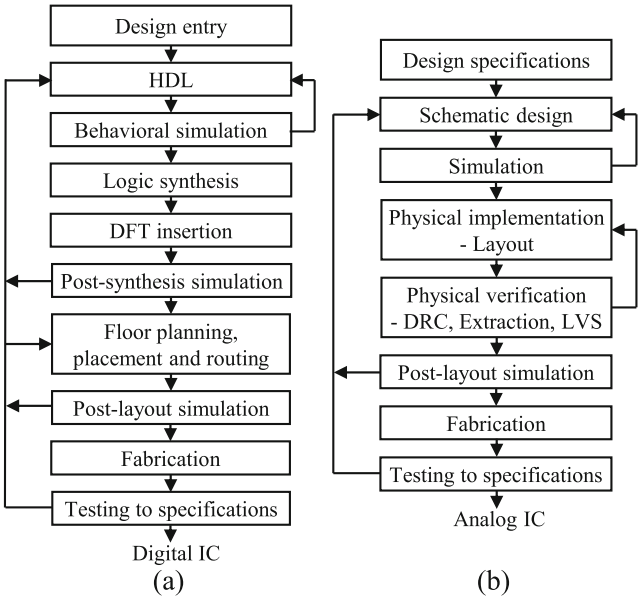

Fig. 2 Design flow of **a** digital IC and **b** analog IC

and design-for-test (DFT) circuits are inserted which are used to facilitate the testing process. Next, post-synthesis simulation verifies the design specifications. Floor planning, placement, and routing of the design are often semi-automated. The rest of the flow is similar to analog IC design flow. The reality of an IC development is much more complex and includes many iterations through various portions of this flow until the final design converges to a form that meets the specification requirements. Design automation can reduce this effort and plays a critical role in designing a complex IC.

As discussed above, the digital and analog IC design flow is different, and the major distinctions can be summarized as follows:

- *Simulations*: Digital circuits are simulated at the gate level, but in analog circuits, simulations are performed at the transistor level.
- *Design specifications*: AMS ICs contain more specification parameters compared to digital ICs such as throughput, linearity, bandwidth, gain, noise, and more.
- *Flexibility in design and synthesis*: Digital design flows contain automatic synthesis processes based on hardware description languages. AMS IC designs follow a less systematic design, where automatic synthesis may not be available, the design is typically time-consuming, and it depends heavily on designer's experience.
- *Structural and functional complexity*: Analog circuits are functionally more complex, while digital circuits have higher structural complexity.

- *Sensitivity to crosstalk, noise, and process variations*: AMS ICs suffer from high sensitivity to crosstalk, noise, and process variations.
- *Testing procedure*: Digital IC testing is predominantly structural, uses standard fault models, and often requires embedded DFT circuits. On contrary, AMS IC testing procedure is predominantly functional and, in most cases, does not have any standard fault model.
- *Fault-free/faulty circuits*: It is comparatively easy to identify the fault-free/faulty circuits in digital ICs due to standard DFT. Identification of fault-free/faulty circuit in AMS ICs depends on tolerance values of AMS specifications and makes the distinction process harder.
- *Verification*: IC performance is verified in multiple domains in AMS circuits.
- *Custom design*: Generally, AMS ICs use full/semi-custom design where designers may not use predefined cells.

Design and test flows can help to understand electrical tests for counterfeit detection, and how to the insert and detect hardware Trojans.

3 Analog and Mixed Signal-Enabled Security: Challenges and Opportunities

Over the last decade or so, globalization has resulted in a tremendous increase in vulnerabilities within the IC supply chain. A lot of research has been conducted on securing the supply chain resulting in security features like IC identification and authentication using PUFs, IC obfuscation and locking, and data encryption. However, they are developed only for digital ICs and cannot directly be extended to AMS ICs. Analog realization of digital concepts requires a large area and is not always feasible [12]. Moreover, cryptomodule consumes a great amount of power and memory which are not available in many applications, such as IoT sensors and smart cards. Many larger systems such as smart grid, smart meter, and industrial control system [14] mainly contain analog components and need secure communications for authentication and tamper monitoring in physical systems. In addition, the lack of analog cryptomodule creates a major problem in applying security features, e.g., hardware IP metering, secure split test (SST) to analog and mixed signal circuits. Thus, the concepts of using analog devices in designing cryptomodule become essential.

In this section, we discuss analog-based security features, PUF, and chaos-based cryptography that can address the security vulnerabilities discussed above. Motivations, challenges, and possible research directions of these features are provided for better understanding.

3.1 Suitable Analog PUF

3.1.1 Motivation

As the number of networked smart ICs, user data, and the counterfeit device is increasing, demands to ensure the security and reliability of these units and their corresponding systems are equally growing. One of the major tasks lies in realizing secure methods of IC identification and authentication. The traditional methods rely on secret digital keys stored in on-chip nonvolatile memory, which are vulnerable to cloning and hacking. PUF can eliminate these vulnerabilities by providing a volatile, unique, tamper-resistant key/ID by utilizing the silicon random process variation. They can be categorized into weak and strong PUFs.

Weak PUFs provide a method based on random disordered physical medium fluctuations and have very few, fixed challenges (inputs), commonly only one challenge per PUF instance. Strong PUFs also leverage process variation of the ICs and extract unique responses. However, they allow a lot of possible challenges and therefore produce a larger number of responses. Weak PUFs, in general, generate a single response and are suitable for identification. To the contrary, strong PUFs allow free querying of their responses and strengthen the authentication process.

Most PUFs are designed and implemented using digital logic, often requiring large area and power. Thus, AMS ICs cannot always take advantage of them. In contrast to digital logic, analog circuits work on a broader spectrum of output. For instance, digital logic contains logic “0” or “1” but analog output can be versatile. For instance, the outputs of AMS ICs are not only digital bits but could be current and voltage.

3.1.2 Existing Analog PUFs

A fully static and monostable current mirror-based PUF has been implemented in [15] that amplifies the random transistor mismatch through two complementary current mirrors and uses sense amplifier. The PUF architecture was fabricated in 65-nm technology and provides standard quality in terms of uniqueness ($\sim$ 0.5), bit instability (2% at nominal condition), and bit bias ($\sim$ 0.5). Li and Seok [16] designed and fabricated PUF based on analog circuits in 65-nm technology node whose output is proportional to absolute temperature (PTAT) current. Csaba et al. [17] investigated cellular non-linear networks that consist of dynamical arrays of locally interconnected cells. This paper argued that analog circuits yield higher security than digital ones in general. R-2R ladder digital-to-analog converter (DAC)-based PUF has been proposed and simulated in [18]. The design relies on the non-linear characteristics of the

analog voltage generated by R-2R ladder DAC. Mixed signal ICs can take advantage of ADC- and DAC-based PUFs. Bryant et al. [19] presented a novel PUF by employing the offset voltage mismatch of the comparators used in a stochastic analog-to-digital converter (ADC) that minimizes the hardware area overhead.

A low-power current-based strong PUF with a hundred of challenge-response pairs was introduced by Majzoobi et al. [20]. The proposed PUF uses a linear combination of current and converts the analog variations present in device leakage current to unique digital responses. PUF based on the exponential current-voltage behavior in the subthreshold region of FET operation has been introduced in [21]. This design derives nonlinearity from the exponential dependence of current on subthreshold voltage. Analog push-pull amplifier PUF is presented in [23] for digital and mixed signal ICs. This PUF exploits the process variation, nonlinearity, and memory effects of the amplifier with the help of ADC and DAC component.

3.1.3 Limitations/Challenges

Although there are few analog PUFs, none are low cost or small enough in size for analog ICs. The reliability issues of PUF are also still a great concern as the response changes with the environmental variations and aging of the device. Generally, error-correcting code (ECC) is used to ensure reliable PUF output, but ECC is a digital concept and usually takes large area; thus, it is not always feasible for AMS ICs. PUFs require additional pins to receive the challenge and to transmit the response. Since additional pin counts increase the cost, it becomes difficult for a designer to include a PUF in AMS ICs. In contrast, additional pins do not increase much cost for digital ICs since they have far more available. In case of strong PUF, most of the work does not discuss the challenge circuit that could potentially increase the overall area.

3.1.4 Opportunities

In contrast to digital logic, analog circuits cover a broader spectrum of input and output. For instance, digital logic contains logic "0" or "1" but analog input and output are more versatile. As a result, analog circuits can provide additional opportunities for generating challenge-response pairs. For example, analog PUFs can take advantage of the memory effect and nonlinearity in analog circuits. Along with physical variation, memory effect and nonlinearity can act as entropy sources and increase the unpredictability of the PUF response. Such possibilities were utilized by Chen et al. [22] and Deyati et al. [23] to design cellular nonlinear networks and PUFs, respectively.

3.2 Chaos-Based Cryptography

3.2.1 Motivation

Cryptomodules are the essence of most of the security primitives. Lack of analog cryptocircuits such as encryption or decryption modules limits the possibility of analog-enabled security primitives. In case of digital ICs, encryption or decryption circuit takes large area. Thus, a low-cost and small area cryptomodule is desired not only for AMS ICs but also for digital ICs. Chaotic circuit-based cryptography is a promising candidate to overcome the deficiency of conventional cryptography. Chaotic circuits are implemented with a few analog components. They generate aperiodic behavior in a deterministic and nonlinear fashion that is highly sensitive to initial conditions and circuit parameters. The behavior of a chaotic system becomes difficult to predict without any prior knowledge of the organization. These phenomena can be compared with key-dependent confusion and diffusion in cryptography. Although chaotic cryptography is not considered suitable for applications with high security demands, it can be an adequate, lightweight solution for AMS-enabled features.

Another important block in most of the cryptographic applications is random number generation. It is used as one-time use numbers (nonces), random seeds, temporary keys in secure communications, secured servers, and processors. Chaotic circuits can provide low-cost, small area solutions in this regard since chaos circuits may be implemented with a few analog components.

3.2.2 Existing Works

The fundamental items in a cryptosystem are data encryption, decryption, and key management. Chaotic cryptosystems containing these items are illustrated in Fig. 3. During transmission, the plaintext is encrypted using cipher key obtained from the chaotic generator. When receiving, the encrypted ciphertext is decrypted using the cipher key generated by the chaotic circuit. It is assumed that chaotic generator in both transmitter and receiver produce the same cipher key.

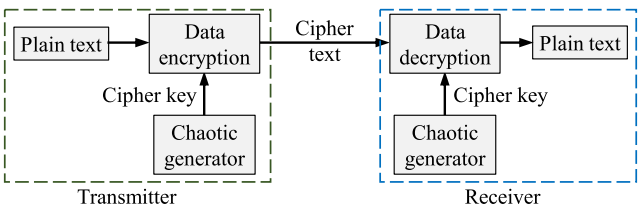

Fig. 3 Basic structure of chaos-based encryption and decryption [24]

In many chaos-based secure communication systems, the cipher key can be made from chaotic circuit parameters and initial conditions given that chaotic behavior is not compromised [25]. Thus, the initial conditions and the circuit parameters play the role of the secret key for encryption. Data encryption includes chaotic masking (addition of plaintext to the cipher key), chaotic modulation (the plaintext modulates a parameter of the chaotic generator or multiply the cipher key), chaotic switching, or chaos shift keying (plaintext is used to choose the signal from two or more different chaotic generators). Generally, receiver systems consist of chaos synchronization technique [26]. It means that two chaotic systems can synchronize with each other under the driving of one or more scalar signals, which are generally sent from one system to another. A hardware implementation of such system was demonstrated [24]. Chaos shift keying (CSK) methods have been explored for secure communication [27, 28]. The communication system using chaotic modulation scheme called modified differential chaos shift keying was implemented in 0.25-μm CMOS technology [27]. Figure 4 depicts the architecture of this system. Here, a reference chaotic waveform is transmitted during the first half of each bit period of plaintext and modulated in the remaining half. At the receiver, the signal is delayed by half a bit period and correlated with the undelayed signal to get the decision variable for producing the output data stream. This process does not need synchronization, but it does not offer as much security.

The general structure of a true random number generator (TRNG) consists of an entropy source and a sampling circuit to extract the entropy. A quality TRNG extracts maximum entropy from the source and becomes a statistically independent and unpredictable sequence. Nonlinear dynamical systems operating in chaotic regime can be used as an entropy source as shown in Fig. 5. The chaotic systems are sensitive to initial conditions, i.e., a small perturbation eventually causes a large change in the system state. With such initial uncertainties, the system's behavior can be

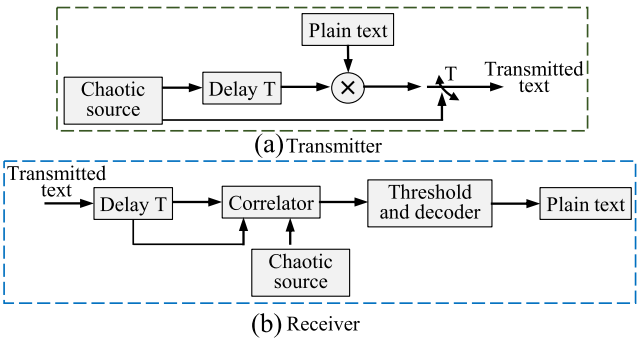

Fig. 4 Chaos shift keying-based communication [27]. **a** Transmitter. **b** Receiver

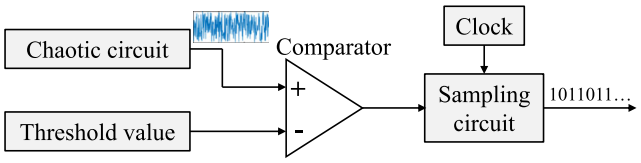

Fig. 5 Random number generation using chaotic circuit

predicted only for a short period. If the chaos-based system is well designed, the output of the system becomes unpredictable. Different types of chaotic behavior including double scroll, piecewise-linear, and Chebyshev map have been studied in prior work [29–31]. Hardware implementation of a switched-current circuit-based chaotic algorithm is presented in [30] to generate a wide-band random number. This work used 0.25-μm CMOS process to carry out the proposed design and statistical method to verify the performance. In [31], field-programmable gate array (FPGA) implementation of continuous time chaotic oscillator is utilized to obtain random number. Katz et al. [29] demonstrated a differential current mode chaos circuit to generate robust random number in 90-nm CMOS-SOI technology that passed the FIPS 140.2 statistical test.

3.2.3 Challenges

Although there are several proposed works for chaos-based cryptography, most of them lack IC implementation. While software applications of chaos cryptosystems are available [32], hardware implementation is provided by very few works [24, 27]. The implementation of cryptomodule using analog circuitry is required to understand the proper behavior of the circuit. Generating the same cipher key in both transmitter and receiver is a challenge due to process, temperature, and noise variation of the systems.

One of the primary concerns of any cryptosystem is security. It is usually assumed that algorithm and cryptosystem are known to all and key is secret. In chaos-based cryptosystem, the secret key includes circuit parameters and initial conditions. Thus, a detailed security analysis should be performed.

Although a few chaos-based random number generation showed good statistical result, robustness against temperature, and supply voltage variation, noise is not yet highly explored. Prior works described in this paper indicate that chaos-based circuit with small circuits may be able to provide a low-cost, lightweight solution.

3.2.4 Opportunities

Cryptomodules are the essential element of modern systems for protecting sensitive materials and communication.

Traditional cryptomodules require a large amount of hardware (registers, control logic, logic gates, etc.), making them particularly less attractive for smaller, less complex AMS ICs. Chaotic cryptography takes advantage of the complex behavior of chaotic dynamics to hide or mask information. Signals resulting from chaotic dynamics are broadband and present random-like statistical properties. Moreover, it requires a small area as it contains a few discrete elements and circuits (e.g., resistance, opamp). Prior works described in this paper indicate that chaos-based circuit may be able to provide a low-cost and lightweight solution. However, the security of chaos has not been thoroughly investigated, thus providing an opportunity for future work.

4 AMS Counterfeit ICs: Challenges and Opportunities

IC counterfeiting is a long-standing problem with non-trivial impacts on many sectors. Consequently, counterfeit detection has received considerable attention from researchers. While most of this work has been focused on digital ICs, AMS ICs are in fact the most widely reported counterfeited parts among all types of popular semiconductors [8]. Counterfeit IC reports from 1985 to 2013 created by Government-Industry Data Exchange Program (GIDEP) [33] and White Horse Laboratories (WHL) [34] include amplifiers, converters, voltage regulators, ADC, DAC, and sensors. Original component manufacturers (OCMs) with counterfeit parts from these sources include TI, Analog Devices, Fairchild, National Semiconductor, Maxim, Freescale, and Motorola. Table 1 shows the types of analog and mixed signal ICs that appeared most frequently in these reports. Figure 6 shows the frequency of counterfeit AMS components by manufacturing year. ICs manufactured between 2000 and 2011 are more often reported as counterfeit. Given the difference in packaging technology and power supply requirements before 2000, it would be difficult and not financially beneficial to the counterfeiter to counterfeit such outdated chips. Components manufactured after 2011 are easier to purchase from authorized distributors and less likely to be harvested from used systems; thus, the number of reported incidents makes sense.

In general, AMS ICs are easier target for several reasons:

- Analog components have long life cycles (in some cases decades), which works better for long-term counterfeiting success.
- Digital designs are large, complex, and more difficult to reverse engineer whereas analog designs are typically single function on a small die. Small companies or individuals can reverse engineer the IC easily with an intermediate-level lab setup.

Table 1 Frequently reported counterfeit AMS ICs in GIDEP and WHL reports

Analog ICs	Mixed signal ICs
Amplifiers	ADC and DAC
Converters	Transceiver
Analog Mux	Timer/oscillator
Motor control	DDS modulator
SMPS	Transmitter
Voltage regulator	Filters
Overvoltage protector	Frequency synthesizer

- Competition among digital IC manufacturers drives profits down whereas analog margins are high. Thus, counterfeiters can undercut the competition by selling AMS ICs at low prices while still netting large profits.
- The number of major markets (automotive, computer, mobile, etc.) using AMS ICs is larger [8].
- Analog lithography is 0.18 μm or larger, so ICs are more easily cloned using older and less expensive facilities.

In this section, we discuss the details of counterfeit AMS ICs that include counterfeiting types, limitations of existing detection, and avoidance measures in analog and mixed signal domain, and provide possible research directions.

4.1 Counterfeit IC Types

A taxonomy of counterfeit ICs is presented in [1]. A similar taxonomy can be used for AMS ICs (see Fig. 7). *Recycled* parts are used components reclaimed or recovered from a system (e.g., e-waste) and modified to be misrepresented as a new component. Such ICs are prone to failure due to their prior usage and reclaiming process involving high temperature, aggressive physical removal, etc. Unreliable recycled ICs should not be used in critical applications. *Remarked* parts refer to components whose legitimate manufacturer markings have been replaced with forged markings without the authorization of the manufacturer. The primary

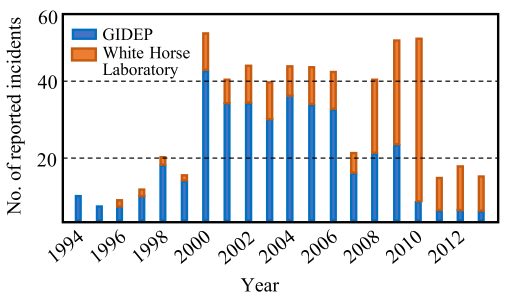

Fig. 6 Frequency of analog and AMS ICs reported as counterfeit compiled from GIDEP and WHL reports

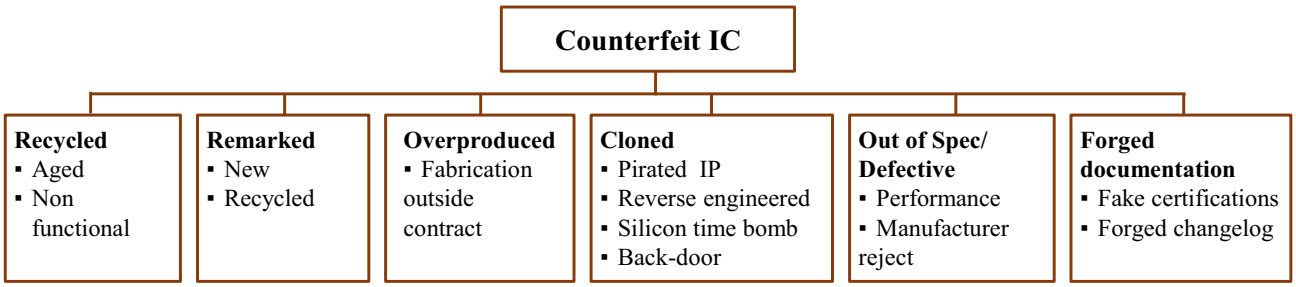

Fig. 7 Classification of counterfeit ICs [1]

incentives for remarking are to drive up a part's price on the open market by upgrading a lower grade part to a higher grade or to make a dissimilar lot fraudulently appear homogeneous. *Overproduction* occurs when an untrusted foundry/assembly (who has access to a designer's intellectual property) fabricates/assembles and then sells parts in the open market outside of its agreement with the design house. *Cloned* parts are unauthorized copies made by parties without the legal IP rights to produce the part (e.g., through reverse engineering, unauthorized knowledge transfer). Since cloned ICs come from untrusted authority, it may contain malicious hardware that interrupts its normal operation and/or disables it in the future, effectively making it a silicon time bomb or create a back door that gives access to critical system functionality. *Out-of-spec/defective* parts are those parts that should be destroyed since they fail post-manufacturing tests, do not meet specifications, etc., but are instead sent to market. *Forged documentation* occurs when a part's associated documents, e.g., specifications and testing, are illegally modified to misrepresent the information about the part.

4.2 Existing Detection and Prevention Approaches

The detection of counterfeit ICs refers to identifying counterfeit parts that are already in IC supply chain. The avoidance measures are taken to prevent counterfeit parts from entering supply chain [1]. Researchers proposed many detections and avoidance techniques due to multifaceted nature of counterfeiting. Existing approaches related to prevention and detection of counterfeit ICs can be divided into three categories: physical inspections, electrical tests, design for anti-counterfeit (DfAC). Physical inspections and electrical tests are appropriate for legacy and active ICs. Legacy components are no longer manufactured by the OCM. Newer designs or new technology nodes may replace the legacy ICs to improve performance, reliability, and/or manufacturing cost. Active components are still being manufactured by OCMs, but their designs cannot be changed because of the additional cost for the new mask as well as performance and reliability concerns. As a result, active and legacy ICs do not present opportunities to add DfAC techniques. New ICs are yet to be designed, thus permitting DfAC techniques.

4.2.1 Physical Inspection

Physical tests are performed to examine the physical and chemical/material properties of the component's package, leads, and die to detect counterfeit defects. Counterfeit defects are anomalies and changes that are not typically found in authentic parts. Common anomalies include wrong markings in package, dents, and reworked leads, missing bond wires, and wrong die [1]. As part of the physical inspection procedure, the component's interior and exterior are thoroughly inspected using imaging techniques [35]. Common imaging techniques include X-ray, scanning electron microscope (SEM), and tomography.

While physical tests are applicable to analog, digital, mixed signal ICs, they require long test time and high costs. In today's global electronics supply chain, counterfeit ICs need to be detected quickly, non-destructively, and inexpensively. Physical inspection does not fulfill any of these needs. Physical tests are destructive in some cases, rely on trained subject matter experts, and lack effective quality metrics for evaluation and automation. In addition, sophisticated counterfeit components having visual properties as good as original components can pass physical test methods. They also do not cover all the counterfeit IC types. It is only effective for recycled, cloned, and remarked ICs. Golden/reference data (e.g., package type, lead frame and bond configuration, material properties) from known components are required for cloned IC detection.

4.2.2 Electrical Tests

The electrical tests are divided into general electrical and targeted electrical tests. *General electrical tests* are used to capture IC and device parameter distributions and compare them to the device specifications. Open circuit, short

circuit, parameter specification tests are common general tests. Both digital and AMS ICs can take advantage of the test process. Given the wide range of part types in the market with different pin counts, functionalities, etc., it is difficult to perform these tests in practice. In addition, they are restricted mainly to the detection of out-of-spec/defective and remarked counterfeit types.

Targeted electrical tests have been developed by academia recently to detect recycled ICs. These tests target the specific electrical property of the chip and compare it with reference chip data. For example, the degradation in electrical parameters due to aging is exploited to detect recycled ASICs and FPGAs [36–38], and comparison of electromagnetic emission from aged and unused chip can be used to identify used components. The challenge, however, is that measurements from known unused ICs must be available for comparison. In addition, the testing process requires different specialized equipment, algorithms, and test programs for each of the digital and AMS component types.

Many techniques require access to golden (i.e., known authentic) measurements, designs, or specifications, which are typically not available. With the large volume of the IC type, it is hard to maintain the information of every manufactured chip. In some cases, such as in legacy ICs, there might not be any available information to generate a complete set of test vectors to test a legacy chip in archived records at the OCM. Generally, electrical tests (open circuit, short circuit, etc.) can help to detect recycled components, but they are ineffective in most of the cases as ICs can be properly functional. There is only one targeted electrical technique [39] for AMS ICs, which estimates the age of the analog ICs using a statistical methodology and detects the recycled ICs. It requires an accurate simulation model of the entire design to determine the age of the design, which may be overshadowed by the process, power supply, and environmental variations.

Not all counterfeit types are adequately covered by electrical tests. For example, overproduced and cloned ICs will avoid detection as long as their electrical parameters and performance remain within the component specification.

4.2.3 Design for Anti-counterfeit

Avoidance measures can be introduced in new ICs by modifying or adding prevention logic. Common avoidance techniques proposed by researchers include PUF, combating die and IC recycling (CDIR), and hardware metering.

- *PUF*: A PUF is a circuit that when interrogated by a challenge (input), it generates a unique device response (output) that depends on the manufacturing variations experienced by the PUF. PUF responses have been utilized to generate unclonable chip IDs to identify and authenticate the chip. Thus, it can prevent overproducing and cloning of ICs.

  As mentioned in analog PUF description, most of the PUFs are designed using digital logic. There are few works in AMS ICs, but they require a large area. For small size AMS ICs, practical realization of PUF is not economically feasible. A common problem with all the PUF is the reliability issue that is yet to be fully addressed [40]. One way to make PUF output reliable is error-correcting code (ECC), but that is fully digital. Thus, an analog realization of ECC scheme is not practically feasible.
- *CDIR*: Embedded aging sensors (i.e., silicon odometer) are proposed for new ICs to detect the usage time. Low-cost embedded sensors/structures called CDIR [41] were implemented to detect recycled counterfeit ICs. The most common CDIRs are based on self-referencing between two ring oscillators (ROs). One of the ROs is a "reference" RO that is protected from aging. The second RO is always running so that it ages more rapidly and becomes slower over time. By comparing the frequency of these two ROs, a statistical decision about aging time can be made.

  For analog and mixed signal (AMS) ICs, the additional control logic here is a challenge as running the stressed RO at high frequency will consume large power and generate considerable noise in the surrounding circuitry. CDIR also requires extra pin circuitry to measure the output. For small analog ICs, creating an extra pin increases the cost.
- *Hardware metering*: Hardware metering approaches are developed for large digital ICs to provide design house the post-fabrication control of the ICs over foundry. The basic idea behind the existing approaches for preventing overproduction is shown in Fig. 8. Two major components are obfuscation-based locking [42] and asymmetric encryption. In this way, the IP owner can

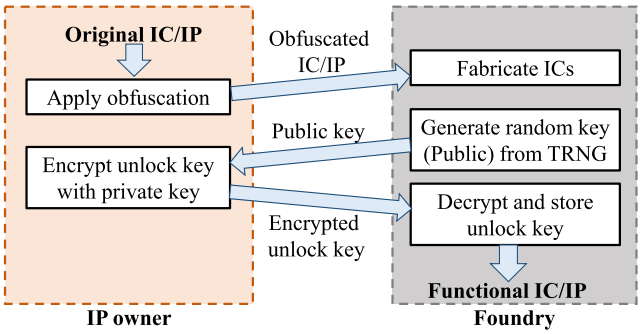

Fig. 8 Hardware metering technique

determine precisely how many keys are given to the foundry/assembly, thereby preventing overproduction. Ideally, there are two elements needed for hardware metering schemes. First, a key management scheme is needed to accept, store, and apply an unlocking key to the manufactured chip. In other words, it is responsible for protecting the IC design from being copied, overproduced, or used without complete understanding of the base design. Second, an obfuscation approach is responsible for protecting the IC design from being reverse engineered and for protecting the key management portion from being trivially removed/attacked. There have been only a few works in analog IP obfuscation. Current and voltage biasing circuits have been used in obfuscating analog IP in [43]. A configurable current mirror method has been proposed by [44] to obfuscate analog IP. This work uses satisfiability modulo theories to generate the locking keys for obfuscated IP where a single key value can make analog IC operate properly while the other key values result in performance degradation or malfunction. In conjunction with on-chip PUF response, IP owner key can unlock the obfuscated circuit. Here, the challenge is that multiple keys may provide operating condition close to the proper behavior of analog circuit block.

Hardware metering is only applicable for large digital ICs as it requires huge area overhead. Since obfuscation and encryption are digital concepts, the analog realization of digital hardware metering is not always feasible. Thus, the design is not applicable to analog ICs. While it may be possible to add such logic to mixed signal chips, the overhead would be prohibitive for most of the ICs.

In the above hardware metering technique, untrusted foundry/assembly can hide yield and supply defective/out-of-spec ICs. To prevent that, secure split test (SST) was developed for large digital ICs to allow IP owners to reassert control over foundry and assembly [11, 45]. SST techniques can prevent that by maintaining a protocol between IP owner and foundry/assembly as shown in Fig. 9. In fact, SST is the only technique that can prevent out-of-spec/defective ICs. Here, IP owner sends the design to the foundry, and foundry fabricates ICs and sends back the TRNG value from the ICs. IP owner modifies and encrypts the TKEY and sends it to the foundry. By applying the TRNG, foundry will get a perturbed response. IP owner can verify the response along with the help of TRNG and mark the IC as pass/fail. The passed ICs are unlocked by the FKEY generated by the IP owner that is unique for each chip. SST also requires encryption and IC locking logic that are only available in digital domain. Thus, the design is not applicable to analog ICs.

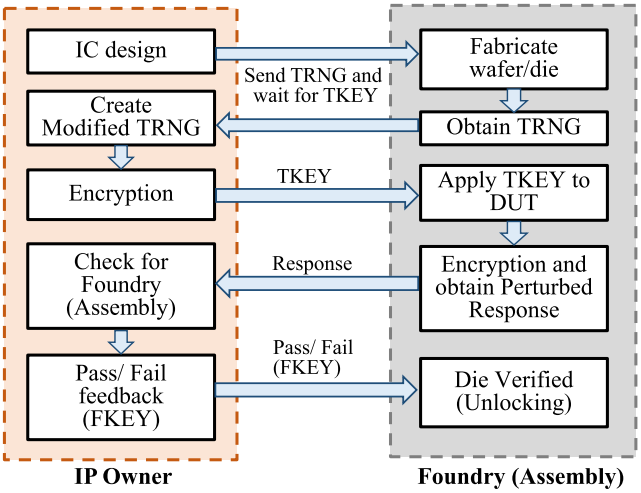

Fig. 9 Basic architecture of secure split test (SST)

4.3 Summary of the Limitations and Challenges in AMS Counterfeit IC Detection and Avoidance Techniques

In Section 4.2, common counterfeit detection and prevention techniques are discussed. Most of the techniques were developed in digital contexts and, in general, are not directly applicable to AMS ICs. The limitations of these approaches are discussed below.

i. *Does not cover all counterfeit types*: The existing techniques do not adequately cover all counterfeit types of AMS ICs, as shown in Table 2. Most notably, overproduced AMS ICs cannot be detected or prevented by any technique.
ii. *Time and cost constraint*: Physical inspections and general electrical tests are time-consuming and costly as shown in Fig. 2. Physical inspections are sometimes destructive, thus not always viable.
iii. *Lack of golden data*: Electrical tests and a few physical tests require golden data from known reference component. Sometimes, golden data are hard to obtain, i.e., information is not always available for legacy ICs. In addition, the number of active ICs is very large; thus, maintaining information of them is not always feasible.
iv. *Impact of process variation*: Electrical test result suffers from manufacturing process variation that overshadows the aging/anomaly behavior.
v. *Lack of logic implementation and memory in AMS*: DfAC techniques require digital logic and memory for obfuscation, encryption, etc. be added to the ICs. Digital realization of these security features in analog ICs are not always feasible [46]. For example, cryptography features cannot be realized by analog block.

Table 2 AMS IC detection and avoidance techniques for each counterfeit IC type

Counterfeit types	Detection techniques	Golden IC/spec	Time/cost	Applicable for digital IC only?
	Physical inspections	No	High/high	No
Recycled	Targeted electrical tests	Yes	Low/high	Yes
	Physical inspections	No*	High/high	No
Remarked	General electrical tests	Yes	High/high	No
Cloned	Physical inspection	Yes	High/high	No
Overproduced	None	N/A	High/high	Yes
Out-of-spec/defective	General electrical tests	Yes	High/high	No

*Might be

Implementing these security features is costly in terms of the required gate counts and secured memory and thus may not be economically attainable.

vi. *Additional pin cost in AMS*: The additional pins needed for DfAC techniques are often not available in small analog ICs. AMS chips have the limited number of pins (e.g., some can have as few as three pins). Original chip manufacturers do not want to increase the pin count as the price of the package will increase, the footprint will change, and it will not be compatible with legacy chips in the same fabrication line.

vii. *Low price of AMS ICs*: A great portion of analog ICs consists of few gates and their prices are low. Introduction of DfAC techniques into them increases the area and cost. For instance, PUF used for identification requires a good number of gates based on the number of response bits, and the addition of a PUF in a small analog IC increases the total gate count tremendously.

4.4 Opportunities in AMS Counterfeit Research

The limitations and challenges of the counterfeiting detection and avoidance techniques in AMS circuit arise mainly due to the small size and limited functionality of AMS ICs. Hence, countermeasures should be realized according to size and integration types. Lightweight, low-cost solutions are more applicable to stand-alone ICs while embedded/SoC ICs can afford most costly detection or avoidance features. We divided the probable solution techniques into stand-alone and embedded/SoC categories and considered counterfeit IC types as shown in Table 3.

- *Recycled*: Recycled ICs are the most common in the counterfeit market and demand considerable attention in detection and prevention techniques. Physical inspections methods are more appropriate where ICs will be used for critical applications since they are time-consuming and costly. The representative behavior or functionalities of the stand-alone AMS ICs can be used for targeted electrical tests as recycled ICs are aged and show different characteristic behaviors than unused ICs. For instance, electromagnetic emission from the aged and unused low drop-out (LDO) voltage regulator, DC to DC converter, and opamp [48, 49] are different and can be utilized to detect recycled component. An effective solution using targeting electrical tests can be achieved by taking advantage of common circuitry found in all analog and mixed signal ICs, such as low drop-out regulators (LDOs). The technique can measure the characteristics of LDOs present in the ICs and make the decision about the IC status. In the case of embedded/SoC system, it is hard to perform the test targeting only the AMS ICs. For new ICs, it is possible to design low-cost analog CDIR that can serve as the prevention technique in AMS IC design.
- *Remarked*: The major differences among commercial, military, and industrial grade chips are operating temperature range, radiation tolerance, packaging, and reliability. These characteristic behaviors can be used for targeted electrical tests. High-grade chips are costly, so an addition of analog PUFs for identification and authentication might be reasonable. Weak and strong PUFs can be applied to stand-alone and embedded AMS ICs respectively to minimize the cost.
- *Cloned*: Cloned counterfeiting can be prevented by low-cost PUF and electric chip ID (ECID). Weak analog PUF can provide unique ID for stand-alone ICs. Embedded/SoC chips can take advantage of digital PUF.
- *Overproduced*: Hardware metering to prevent overproduction might be addressed by low-cost chaotic cryptography (described in Section 3.2). Although metering approaches for AMS chips have been proposed recently, they only focus on the portions of the key management scheme. This is partially due to the challenges associated with obfuscating analog circuits. In the digital circuits, the obfuscation involves masking of boolean functions and logical values. However, since analog circuit operations depend on a continuous range

Table 3 Probable AMS IC counterfeit detection and avoidance techniques

Types	Stand-alone IC	Embedded/SoC
Recycled	Analog CDIR, targeted electrical tests*, physical inspections	Analog CDIR, physical inspections
Remarked	Targeted electrical tests*, analog PUF	Targeted electrical tests, analog CDIR, PUF
Cloned	Weak PUF, ECID	PUF, ECID
Overproduced	Analog hardware metering	Hardware metering
Out-of-spec/Defective	General electrical tests	

*Might be possible

of input/output values, there is an increased complexity when obfuscating analog blocks. Moreover, analog circuits are tightly designed within parameter bounds aiming specific gains, phase noise, bandwidth, etc. Therefore, any added circuitry may cause large shifts in the output parameters. Biasing circuits are critical circuit block to establish the proper operating conditions and can be considered separate from functional circuit block. Thus, current and voltage biasing circuits are good candidates for obfuscation as shown in [43, 44].

- *Pin-less CDIR and PUF measurement*: Limited number of pins in AMS ICs creates a major barrier in PUF and CDIR implementation. Therefore, it is essential that access/read of the PUF or CDIR data be accomplished without adding any extra pin to the design.

5 Analog and Mixed Signal Hardware Trojans: Challenges and Opportunities

ICs are vulnerable to hardware Trojans due to the globalization of the semiconductor IC supply chain and reliance on third-party intellectual property (IP) as well as external fabrication processes. A hardware Trojan can be defined as a chip/circuit with the following characteristics:

- Created by untrusted foundry, rogue designer, or third-party IP vendor.
- Designed to be hidden, the probability of which being detected or triggered by existing test and verification steps is very low.
- Contains an intentional anomaly that changes, degrades, or destroys the performance of the circuit or leaks sensitive information.

Hardware Trojans can impose a serious threat to privacy and functional capabilities of real-life systems. Tampering of any IC and changes in circuit structure can stop an IC from working leading to huge economic loss of manufacturing company. Such changes can also alter the functionality of the system and leak important information such as encryption keys to the adversary. In the following subsections, we will describe research on digital hardware Trojans. Then, we will define and categorize Trojans in AMS ICs.

5.1 Digital Hardware Trojans

A detailed overview of hardware Trojans in digital ICs and its taxonomies are provided by [4, 50, 51]. Digital hardware Trojans are classified based on their insertion phase, abstraction level, activation mechanism, effects, and location as shown in Fig. 10. Digital hardware Trojan has mainly two parts: activation mechanism (trigger) and functionality (payload) [52]. A Trojan trigger can be combinational as well as sequential. A combinational trigger can be a very rare activation condition which is highly unlikely to be detected during the conventional manufacturing tests. A sequential activation can occur after a sequence of rare events or after a certain period of continuous operation. A Trojan without activation mechanism is also possible and can always remain active in the circuit. The payload of a Trojan becomes effective after the Trojan gets activated and alters the logic values at the internal nodes of the circuit which can change, degrade, or stop the circuit performance. The research on digital hardware Trojans are broadly categorized into two parts as shown in Fig. 11.

- *Trojan design*: Research on Trojan design mainly includes innovative ways of designing the Trojan trigger and payload such that it is extremely difficult to activate or detect the Trojan. Novel triggers using don't-care states [53] or silicon wear-out mechanisms [54] have been developed which makes the Trojan get triggered in very rare conditions. Added circuitry due to new payloads may cause changes in the characteristics of the whole chip such as power signature and area consumed and may facilitate Trojan detection. Thus, optimizing techniques are employed to optimize Trojan design and avoid easy detection. Different types of Trojan insertion and implementation techniques have been proposed by several research groups. The benchmarks and test vectors analyze the strengths and weaknesses

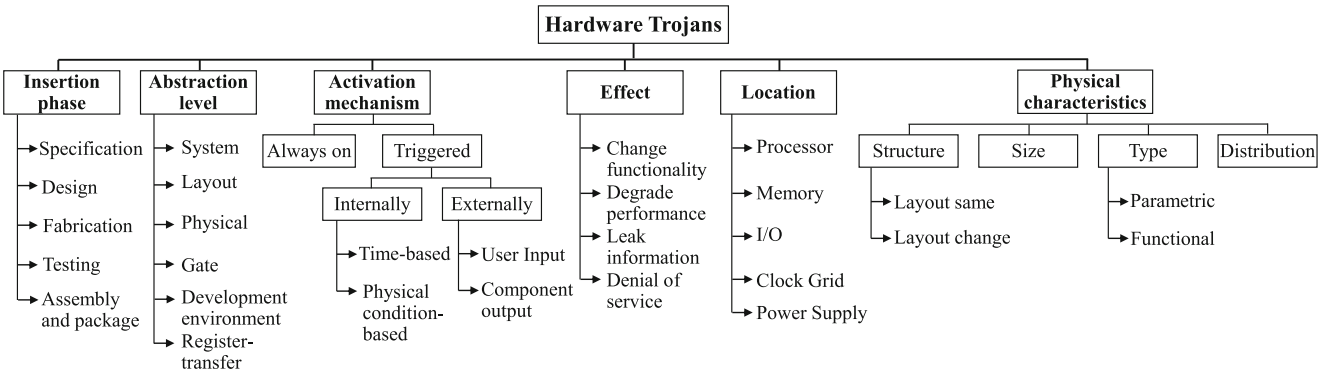

Fig. 10 Taxonomy for digital hardware Trojan [47]

of all these Trojans. Furthermore, to quantify the effect and detectability of a Trojan, some metrics have also been introduced [55].

- *Trojan countermeasures*: The research on countermeasures against hardware Trojans includes validation of existing IC designs either in the design phase (pre-silicon) or after the manufacturing process (post-silicon). Post-silicon methods can be reverse engineering or analysis of power [56], timing [57], temperature [58], etc. signatures of respective ICs. Pre-silicon validation includes functional validation, specification testing, and compliance of circuit area and coverage. Design for trust is mainly associated with creating IC designs with runtime monitoring [58], supportive test points, sensors, and obfuscation [59], within the design which facilitates Trojan detection or prevents Trojan insertion accordingly. Split manufacturing is another technique which aims at building a trusted flow of fabrication process by dividing it into two parts [60],[61]: front end of the line (FEOL) and back end of the line (BEOL) fabrication. An untrusted foundry performing FEOL does not have access to the layers in BEOL and is unable to find the proper part of the IC to insert the Trojan.

The attack models for digital Trojans are shown in Table 4 [5]. These models point out the various possibilities of untrusted sources along the life cycle of a digital chip and show the different ways a digital chip can be attacked for Trojan insertion.

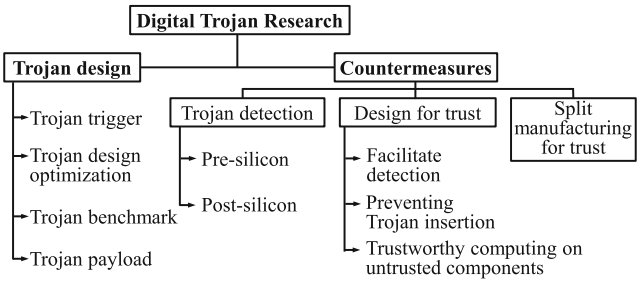

Fig. 11 Overview of digital hardware Trojan research [5]

5.2 AMS Hardware Trojans

Hardware Trojans using analog and AMS circuits drew less attention of researchers compared to digital Trojans. The characteristics AMS Trojans are expected to be different from digital ones due to difference between AMS ICs and digital ICs as discussed in Section 3. Few key points below discuss how the above differences between digital and AMS ICs affect the nature of hardware Trojans in AMS ICs.

- *Possible analog, digital, and mixed signal Trojans in AMS ICs*: As AMS ICs consist of both analog and digital components, a Trojan can have both analog and digital trigger and payloads, and it can originate from the digital part of the IC and affect the analog part or vice versa. The trigger and payload can sometimes both pertain to only the analog/digital part. In order to explore the possibilities, behavior, and effectiveness of Trojans in AMS ICs, it is very important to classify the different kinds of AMS ICs available in the market. We have classified AMS ICs previously in Section 3 in terms of integration. From the classification, we can conclude that Trojans inserted in the stand-alone chips will only have an analog trigger and an analog payload. On the contrary, Trojans included in AMS ICs embedded in SoCs can have all types of possible trigger payload combinations among digital trigger, digital payload, analog trigger, and analog payload.
- *Comprehensive attack models*: A list of comprehensive attack models for digital hardware Trojans is presented in Table 4. But all of these attack models are not applicable for AMS ICs. AMS ICs are smaller and have lesser number of transistors compared to digital ICs. The layout is also custom and compact. Therefore, addition of any Trojan circuitry in the fabrication phase can hurt the performance, matching, and specifications of

Table 4 Comprehensive attack models for digital hardware Trojans [5]

Model	Description	3P IP vendor	SoC developer	Foundry
A	Untrusted 3P IP vendor	Untrusted	Trusted	Trusted
B*	Untrusted foundry	Trusted	Trusted	Untrusted
C	Untrusted electronic design automation (EDA) tool or rogue employee	Trusted	Untrusted	Trusted
D*	Commercial off-the-shelf component	Untrusted	Untrusted	Untrusted
E	Untrusted design house	Untrusted	Untrusted	Trusted
F*	Fabless SoC design house	Untrusted	Trusted	Untrusted
G*	Untrusted SoC developer with trusted IPs	Trusted	Untrusted	Untrusted

*Not applicable for analog/AMS ICs

the whole circuit. If an untrusted foundry manages to implement a perfect additional Trojan circuitry without hurting the performance, the layout is so compact that it will be easily detected. Thus, attack models B, D, F, and G in Table 4 which involve the presence of untrusted foundry are inapplicable for AMS ICs. Due to numerous functions (digital, analog, mixed signal) within a single chip and strict guidelines like FCC guidelines for wireless AMS ICs, it has been a common trend for design houses to purchase third-party IPs. Untrusted third-party IP vendor (model A) can therefore be a major source of Trojan insertion. Apart from this, Trojans can also be inserted during the design phase by untrusted design house (model E) or even by untrusted EDA tools or employees (model C).

5.3 Prior Work on AMS Hardware Trojans

Prior work on AMS hardware Trojans has focused on Trojan design and Trojan detection [64, 66]. A complete framework of the current research in AMS Trojan is shown in Table 5 but a lot more remains to be done. As mentioned earlier, an AMS IC can have all possible trigger payload combinations of digital and analog and none of the current researchers have yet been able to provide a generic formulation of AMS Trojans identifying the various types of trigger payload combinations. In this section, we divide the current state of the art according to Table 5 and discuss the work performed so far.

5.3.1 Trojan Design

The prior works in Trojan design can be categorized as Trojan trigger and payload.

- *AMS Trojan with digital trigger and analog payload*: In [62, 63], Liu, Jin, and Makris demonstrate a Trojan for AMS wireless ICs which originates in the digital part of the IC (digital encryption system) and steals the encryption key through a modified scan chain. The key is then leaked through glitches in the amplitude or frequency of a UWB (ultra-wideband) transmitter and can be decoded from there. This type of Trojan has a digital trigger as it originates in the digital part of the circuit but the payload is analog which is reflected as glitches in the amplitude or frequency of the transmitter.
- *AMS Trojan with analog trigger and analog payload*: Authors in [64, 65, 67] proposed unwanted yet stable DC operating points in few circuits (having more than one operating point) as Trojan states and these can be triggered both in static and dynamic circuits by changing initial conditions or manufacturing process or temperature variations. Once the Trojan is triggered, its functionality can change. For example, a Sallen key band pass filter response changes when stuck in an unwanted equilibrium point. The circuit can even stop functioning, like a Wien bridge oscillator which stops oscillating when it encounters an unwanted state of operation [65]. Although these proposed Trojans have the characteristics of analog Trojans, they are only applicable for a few types of circuits like oscillators, filter [64], bias generators having positive feedback loops [65, 66], and opamps using slew rate enhancement (SRE) circuits [67]. The triggering of such Trojans seems impossible with a start-up circuit already available in most analog/AMS chips which negates the possibility of any unwanted operating states.
- *AMS Trojan with analog trigger and digital payload*: An analog Trojan using the digital circuit as payload is provided by [6]. In this case, an analog capacitor charge sharing circuit with a detector acts as Trojan, and specific registers and instructions are the payload. The detector is designed and fabricated such that it goes undetected during the fabrication process.

For all the above types of Trojans, it is extremely important to implement the malicious effect of the Trojan in real-life examples. For example in [62, 63], the Trojan implemented leaks a key through an analog payload which is malicious. Irrespective of the payload being digital or

Table 5 Tabular overview of analog hardware Trojan research

AMS hardware Trojan research	Description	Types and examples	
Trojan design chain [62, 63]	Trojan trigger	Digital trigger	Triggered in digital encryption standard (DES) with a modified scan
		Analog trigger	1. Analog trigger circuit based on capacitor charge sharing [6] 2. Triggered by unwanted DC operating states in oscillators, filters [64], bias generators with positive feedback loops [65, 66], and opamps with SRE circuits [67]
	Trojan payload	Digital payload	1. Change of functionality: overwrites registers in processors [6]
		Analog payload	1. Leak information: amplitude, frequency glitches in UWB transmitter leak secret key [62, 63] 2. Denial of service: Wein bridge oscillator stops oscillation [65] 3. Change of functionality: response of Sallen key band pass filter changes [65]
Trojan detection	Post-silicon	1. Genetic stimulus evolution model tuning (RAVAGE) [68] 2. On-chip analog neural network [69]	
	Pre-silicon	1. Homotopy/divide and contraction [70, 71]. 2. Graphical [72, 73]	

analog, it must be used for something malicious. If the payload is digital, it is easier to imagine a malicious activity as numerous such examples are proposed by researchers before for digital Trojans. The challenge here is to activate the digital payload successfully with an analog trigger while avoiding detection which shifts the focus to design of the trigger. Examples of using an analog payload to perform something unintended are rarely given in the past; thus, future research must be directed towards design of malicious analog payloads which can be triggered by analog/digital triggers.

5.3.2 Trojan Detection

Unlike digital circuits, analog/AMS has a broad performance range even for a defined operation. For instance, a functional opamp can have $\pm$ 10% variation in its gain, bandwidth, noise, and power and still operate in desired manner (as a stand-alone or as a part of a larger system). In a sense, analog/AMS circuits do not necessarily have a unique response to the functional test. Thus, regular analog testing will not be useful in distinguishing whether a particular analog circuit is faulty or Trojan infested. In other words, a Trojan can be easily disguised in the form of a fault in analog circuits if the response of the same remains within the specification thresholds during regular analog testing. Performance of analog systems covers an extremely broad space in a continuous fashion (currents, voltage, gain, noise, speed, settling, slewing, ripple, phase noise, driving capability, input/output impedance just to name a few) making it much more difficult to detect an undefined response. The payload of an inserted Trojan can affect any of the above parameters which are difficult to cover within a specified test regime. It must not be forgotten that Trojans are always rarely activated which reduces the possibility of it being activated during test time to a bare minimum. The above condition becomes more difficult in case of analog circuits which do not have the luxury of functional testing, automatic test pattern generation (ATPG), etc.

Little work has been done on Trojan detection in AMS ICs. We divide the current state of the art into pre-silicon and post-silicon validations.

- *Pre-silicon*: Pre-silicon approaches only include detection or breaking of the positive feedback loops creating unwanted DC operating points in a few aforementioned circuits. This can be accomplished with graphical methods [72, 73] in which the circuit is converted into a directed dependency graph (DDG). With the help of DDG, a few strongly connected components (SCCs) are identified in the circuit and then graph theory is utilized to detect positive feedback loops and identify the set of node points to be removed. Another theory proposed in [70, 71] explains homotopy methods which convert the circuit into graphical formats with the respective nodes and branches and detect the positive feedback loop (PFL). The PFL is then broken and a voltage source is inserted at the break point which is then swept within a predetermined sweep range to obtain the unwanted DC states (Trojan states). The main drawback of these procedures is that analog Trojan states which have been explained as unwanted operating states can be easily negated by start-up circuits which are readily available

in many AMS chips and which ensure that the circuits maintain the specific desirable operating points. Thus, the probability of such Trojans and even the need for their detection remains low.

- *Post-silicon*: For post-silicon Trojan detection, a model called RAVAGE was proposed in [68] which uses a method of stochastic test generation. The method is stochastic as no knowledge about defects in the device under test (DUT) is known beforehand. This process uses a randomly generated stimulus which aims at maximizing the differences between the behavioral properties of the hardware and a software model while they respond to the same set of stimulus. If a difference between the response of the DUT and the software is noted, then model parameters of the software are optimized and the whole process is repeated. After the end of the optimization process, if there remains a residue which is more than a prior set threshold value, then the DUT is said to have malicious properties. These malicious properties may be or may not be Trojans. Rather, they may simply be bugs or defects. The authors use wireless AMS ICs like up converters and down converters to validate the process. Note that this procedure can be applied for all ICs and is not necessarily to AMS ICs. In [69], another post-silicon trust evaluation method has been described using analog neural network which the end user can use anytime after the IC is deployed in order to examine whether it is trusted or not. The Trojan mentioned has a digital trigger and an analog payload. The detection method can evaluate such Trojans but may fail to detect Trojans with an analog trigger. Thus, the detection processes described till now are not universal and do not cater to the entire AMS Trojan taxonomy.

5.4 Summary of Challenges for AMS Hardware Trojans and Road Map for Future Research

- *Possible ways of triggering a Trojan in AMS ICs*: Although previous research has given a few hints about Trojan states, appropriate Trojan triggers in AMS ICs are still an open problem. Thus, the question remains how can Trojans be triggered in AMS ICs? What are the possible sources of such trigger?
- *Possible payload and effects of a Trojan in AMS ICs*: Keeping in mind that the payload can both be analog or digital, what are the possible effects of a Trojan in an AMS IC? Can these effects be used maliciously by a third party?
- *AMS Trojan taxonomy and benchmarks*: Trojan research in digital ICs has benefited from a clear taxonomy and common set of benchmarks. Because AMS ICs are so different from digital ones, a separate taxonomy and set of benchmarks is needed to study and compare AMS Trojans.
- *Detection metrics of Trojan in AMS ICs*: AMS Trojans may require a unique set of metrics and whole new set of verification tests which fit the AMS test flow.
- *Trojan insertion*: Since analog ICs have low number of transistors (in range of 100s), any addition of transistors may be easily recognized. In addition, with their compact layout, insertion of any additional Trojan circuitry may require redesign. Thus, there remains a big challenge of hiding Trojan circuits in AMS ICs without redesign.
- *Specifying attack models*: Attack models will be different for AMS ICs as we see that insertion of AMS Trojans is not possible in every phase. Insertion of Trojan in foundry or fabrication phase may be inapplicable in AMS ICs as it likely requires redesign and can be easily detected during testing. On the other hand, AMS ICs have numerous third-party (3P) IPs which already meet well-established standards. For example, many wireless AMS ICs utilize 3P IPs from vendors who have already been certified by FCC. Thus, Trojan insertion attacks from 3P IPs, untrusted design house, or rogue employee are still possible for AMS ICs.
- *Real-life examples*: The last challenge is fitting the theory of Trojans in AMS ICs in the practical world. In other words, one must prove that it is possible to insert a well-hidden and easily triggerable Trojan in an AMS IC.

6 Conclusions

In this paper, we presented the landscape of AMS IC security categorizing it into three different aspects: AMS-enabled security, AMS IC counterfeiting, and AMS hardware Trojan. We discussed the prospects of analog suitable PUF and cryptography using the chaotic circuit in analog-enabled security. Although there are few AMS suitable PUFs, none are low cost or small enough in size. Chaos-based cryptography can be implemented with a few analog components and is a potential candidate for low-cost and adequate analog cryptomodule for AMS ICs. The existing counterfeit detection and prevention techniques are developed in digital contexts and cannot be directly applied to AMS ICs. Specifically, additional pins required for detection and avoidance techniques are not often available in AMS ICs. AMS counterfeit IC detection and avoidance techniques for stand-alone and embedded ICs demand different approaches. Hardware Trojans in AMS ICs can take advantage of trigger and payload options from both digital

and analog parts of the circuit, but all the possibilities have not been investigated thus far. Overall, the challenges and opportunities presented in this paper show that there is still a great deal of work needed in AMS security.

Funding Information The authors would like to acknowledge the supports from the National Science Foundation grant (CCSS-1610075) and National Institute of Standards and Technology grant (P0013638).

References

1. Tehranipoor M, Guin U, Forte D (2015) Counterfeit integrated circuits: detection and avoidance. Springer International Publishing
2. Liu B, Gang Q (2016) VLSI supply chain security risks and mitigation techniques: a survey. Integr VLSI J 55:438–448
3. Mishra P, Bhunia S, Tehranipoor M (2017) Hardware IP security and trust. Springer
4. Tehranipoor M, Koushanfar F (2010) A survey of hardware Trojan taxonomy and detection. IEEE Des Test Comput 27(1):10–25
5. Xiao K, Forte D, Jin Y, Karri R, Bhunia S, Tehranipoor M (2016) Hardware Trojans: lessons learned after one decade of research. ACM Trans Des Autom Electron Syst (TODAES) 22(1):6:1–6:23
6. Yang K, Hicks M, Dong Q, Austin T, Sylvester D (2016) A2: analog malicious hardware. In: 2016 IEEE symposium on security and privacy (SP), pp 18–37
7. Guin U, Forte D, Tehranipoor M (2013) Anti-counterfeit techniques: from design to resign. In: 2013 14th International workshop on microprocessor test and verification, pp 89–94
8. Top 5 counterfeited semiconductors: analog ICs top the list—solid state technology (2015). http://electroiq.com/blog/2012/04/top-5-counterfeited-semiconductors-analog-ics-top-the-list/
9. Edward Suh G, Devadas S (2007) Physical unclonable functions for device authentication and secret key generation. In: Proceedings of the 44th Annual design automation conference, DAC '07. ACM, New York, pp 9–14. ISBN 978-1-59593-627-1
10. Forte D, Bhunia S, Tehranipoor MMs (2017) Hardware protection through obfuscation. Springer
11. Rahman MT, Forte D, Shi Q, Contreras GK, Tehranipoor M (2014) CSST: preventing distribution of unlicensed and rejected ICs by untrusted foundry and assembly. In: 2014 IEEE International symposium on defect and fault tolerance in VLSI and nanotechnology systems (DFT), pp 46–51
12. Polianiel I (2016) Security aspects of analog and mixed-signal circuits. In: 2016 IEEE 21st International mixed-signal testing workshop (IMSTW), pp 1–6
13. Quadir SE, Chen J, Forte D, Asadizanjani N, Shahbazmohamadi S, Wang L, Chandy J, Tehranipoor M (2016) A survey on chip to system reverse engineering. J Emerg Technol Comput Syst 13(1):6:1–6:34. ISSN 1550-4832
14. Maxim Integrated, White paper (2013). Energy measurement and security for the smart grid—too long overlooked
15. Alvarez AB, Zhao W, Alioto M (2016) Static physically unclonable functions for secure chip identification with 1.9–5.8% native bit instability at 0.6–1 v and 15 fJ/bit in 65 nm. IEEE J Solid State Circ 51(3):763–775
16. Li J, Seok M (2016) Ultra-compact and robust physically unclonable function based on voltage-compensated proportional-to-absolute-temperature voltage generators. IEEE J Solid State Circ 51(9):2192–2202
17. Csaba G, Xueming J, Chen Q, Porod W, Schmidhuber J, Schlichtmann U, Lugli P, Rührmair U (2009) On-chip electric waves: an analog circuit approach to physical uncloneable functions. IACR Cryptol ePrint Archive 2009:246
18. Pengjun W, Xuelong Z, Yuejun Z, Jianrui L (2015) Design of a reliable PUF circuit based on R-2R ladder digital-to-analog convertor. J Semicond 36(7):075005
19. Bryant T, Chowdhury S, Forte D, Tehranipoor M, Maghari N (2016) A stochastic approach to analog physical unclonable function. In: 2016 IEEE 59th International midwest symposium on circuits and systems (MWSCAS). IEEE, pp 1–4
20. Majzoobi M, Ghiaasi G, Koushanfar F, Nassif SR (2011) Ultra-low power current-based PUF. In: 2011 IEEE International symposium of circuits and systems (ISCAS), pp 2071–2074
21. Kalyanaraman M, Orshansky M (2013) Novel strong PUF based on nonlinearity of MOSFET subthreshold operation. In: 2013 IEEE International symposium on hardware-oriented security and trust (HOST), pp 13–18
22. Chen Q et al (2009) Analog circuits for physical cryptography. In: Proceedings of the 2009 12th International symposium on integrated circuits, pp 121–124
23. Deyati S, Muldrey BJ, Singh AD, Chatterjee A (2015) Challenge engineering and design of analog push pull amplifier based physically unclonable function for hardware security. In: 2015 IEEE 24th Asian test symposium (ATS), pp 127–132
24. Tanougast C (2011) Hardware implementation of chaos based ciphe: design of embedded systems for security applications. Springer, Berlin, pp 297–330
25. Alvarez G, Li S (2006) Some basic cryptographic requirements for chaos-based cryptosystems. Int J Bifur Chaos 16(08):2129–2151
26. Pecora LM, Carroll TL (1990) Synchronization in chaotic systems. Phys Rev Lett 64(8):821
27. Mandal S, Banerjee S (2004) Analysis and CMOS implementation of a chaos-based communication system. IEEE Trans Circ Syst I: Regular Papers 51(9):1708–1722
28. Delgado-Restituto M, Acosta AJ, Rodríguez-Vázquez A (2005) A mixed-signal integrated circuit for FM-DCSK modulation. IEEE J Solid-state Circ 40(7):1460–1471
29. Katz O, Ramon DA, Wagner IA (2008) A robust random number generator based on a differential current-mode chaos. IEEE Trans Very Large Scale Integr (VLSI) Syst 16(12):1677–1686
30. Wang C-C, Huang J-M, Cheng H-C, Hu R (2005) Switched-current 3-bit CMOS 4.0-MHz wideband random signal generator. IEEE J Solid-state Circ 40(6):1360–1365
31. Ergün S, Özoguz S (2005) A truly random number generator based on a continuous-time chaotic oscillator for applications in cryptography. Springer, Berlin, pp 205–214. ISBN 978-3-540-32085-2
32. Kocarev L, Sterjev M, Fekete A, Vattay G (2004) Public-key encryption with chaos. Chaos: Interdiscip J Nonlinear Sci 14(4):1078–1082
33. GIDEP (2015). http://www.gidep.org/
34. White Horse Laboratories (2015). http://archive.constantcontact.com
35. Alam M, Shen H, Asadizanjani N, Tehranipoor M, Forte D (2017) Impact of X-ray tomography on the reliability of integrated circuits. IEEE Trans Dev Mater Reliab 17(1):59–68
36. Alam MM, Tehranipoor M, Forte D (2016) Recycled FPGA detection using exhaustive LUT path delay characterization. In: 2016 IEEE International test conference (ITC), pp 1–10
37. Huang K, Liu Y, Korolija N, Carulli JM, Makrisu Y (2015) Recycled IC detection based on statistical methods. IEEE Trans Comput-Aided Des Integr Circ Syst 34(6):947–960
38. Zhang X, Xiao K, Tehranipoor M (2012) Path-delay fingerprinting for identification of recovered ICs. In: 2012 IEEE International symposium on defect and fault tolerance in VLSI and nanotechnology systems (DFT), pp 13–18

39. Chang D, Ozev S, Sinanoglu O, Karri R (2014) Approximating the age of RF/analog circuits through re-characterization and statistical estimation. In: 2014 Design, automation test in europe conference exhibition (DATE), pp 1–4
40. Rahman TM, Rahman F, Forte D, Tehranipoor M (2015) An aging-resistant RO-PUF for reliable key generation. IEEE Trans Emerg Top Comput PP(1):1–1
41. Guin U, Zhang X, Forte D, Tehranipoor M (2014) Low-cost on-chip structures for combating die and IC recycling. In: Proceedings of the 51st annual design automation conference, DAC '14. ACM, pp 87:1–87:6. ISBN 978-1-4503-2730-5
42. Chakraborty RS, Bhunia S (2009) Harpoon: an obfuscation-based SoC design methodology for hardware protection. IEEE Trans Comput-Aided Des Integr Circ Syst 28(10):1493–1502
43. Rao VV, Savidis I (2017) Parameter biasing obfuscation for analog IP protection. In: International symposium on hardware oriented security and trust (HOST), pp 1493–1502
44. Wang J et al (2017) Thwarting analog IC piracy via combinational locking to appear in International Test Conference (ITC)
45. Contreras GK, Rahman MT, Tehranipoor M (2013) Secure split-test for preventing IC piracy by untrusted foundry and assembly. In: 2013 IEEE International symposium on defect and fault tolerance in VLSI and nanotechnology systems (DFTS), pp 196–203
46. Use analog ASICs to eliminate the threat posed by counterfeit chips (2017). http://anysilicon.com/use-analog-asics-eliminate-threat-posed-counterfeit-chips/
47. Tehranipoor M, Wang C (2011) Introduction to hardware security and trust. Springer Science & Business Media
48. Huang H, Boyer A, Ben Dhia S, Vrignon B (2015) Prediction of aging impact on electromagnetic susceptibility of an operational amplifier. In: 2015 Asia-Pacific symposium on electromagnetic compatibility (APEMC), pp 86–89
49. Wu J, Boyer A, Li J, Vrignon B, Ben Dhia S, Sicard E, Shen R (2014) Modeling and simulation of LDO voltage regulator susceptibility to conducted EMI. IEEE Trans Electromagn Compat 56(3):726–735
50. Karri R, Rajendran J, Rosenfeld K, Tehranipoor M (2010) Trustworthy hardware: identifying and classifying hardware Trojans, vol 43
51. Nahiyan A, Tehranipoor M (2017) Code coverage analysis for IP trust verification. In: Hardware IP security and trust, pp 39–46
52. Chakraborty RS, Narasimhan S, Bhunia S (2009) Hardware Trojan: threats and emerging solutions. In: High level design validation and test workshop, 2009. HLDVT 2009. IEEE International, pp 166–171
53. Dunbar C, Qu G (2014) Designing trusted embedded systems from finite state machines. ACM Trans Embed Comput Syst 13(5s):153:1–153,20
54. Shiyanovskii Y, Wolff F, Rajendran A, Papachristou C, Weyer D, Clay W (2010) Process reliability based Trojans through NBTI and HCI effects. In: 2010 NASA/ESA Conference on adaptive hardware and systems, pp 215–222
55. Salmani H, Tehranipoor M, Karri R (2013) On design vulnerability analysis and trust benchmarks development. In: 2013 IEEE 31st International conference on computer design (ICCD), pp 471–474
56. Agrawal D, Baktir S, Karakoyunlu D, Rohatgi P, Sunar B (2007) Trojan detection using IC fingerprinting. In: 2007 IEEE Symposium on security and privacy (SP '07), pp 296–310
57. Jin Yier, Makris Y (2008) Hardware Trojan detection using path delay fingerprint. In: 2008 IEEE International workshop on hardware-oriented security and trust, pp 51–57
58. Forte D, Bao C, Srivastava A (2013) Temperature tracking: an innovative run-time approach for hardware Trojan detection. In: Proceedings of the international conference on computer-aided design, ICCAD '13. IEEE Press, Piscataway, pp 532–539
59. Chakraborty RS, Bhunia S (2009) Security against hardware Trojan through a novel application of design obfuscation. In: 2009 IEEE/ACM International conference on computer-aided design - digest of technical papers, pp 113–116
60. Vaidyanathan K, Das BP, Sumbul E, Liu R, Pileggi L (2014) Building trusted ICs using split fabrication. In: 2014 IEEE International symposium on hardware-oriented security and trust (HOST), pp 1–6
61. Xiao K, Forte D, Tehranipoor MM (2015) Efficient and secure split manufacturing via obfuscated built-in self-authentication. In: 2015 IEEE International symposium on hardware oriented security and trust (HOST), pp 14–19
62. Liu Y, Jin Y, Makris Y (2013) Hardware Trojans in wireless cryptographic ICs: silicon demonstration & detection method evaluation. In: 2013 IEEE/ACM International conference on computer-aided design (ICCAD), pp 399–404
63. Jin Y, Makris Y (2010) Hardware Trojans in wireless cryptographic ICs. IEEE Design Test Comput 27(1):26–35
64. Wang Q, Geiger RL, Chen D (2015) Hardware Trojans embedded in the dynamic operation of analog and mixed-signal circuits. In: 2015 National aerospace and electronics conference (NAECON), pp 155–158
65. Wang YT, Wang Q, Chen D, Geiger RL (2014) Hardware Trojan state detection for analog circuits and systems. In: NAECON 2014 - IEEE National aerospace and electronics conference, pp 364–367
66. Cao X, Wang Q, Geiger RL, Chen DJ (2015) A hardware Trojan embedded in the Inverse Widlar reference generator. In: 2015 IEEE 58th International midwest symposium on circuits and systems (MWSCAS), pp 1–4
67. Cai C, Chen D (2015) Performance enhancement induced Trojan states in op-amps, their detection and removal. In: 2015 IEEE International symposium on circuits and systems (ISCAS), pp 3020–3023
68. Muldrey B, Deyati S, Giardino M, RAVAGE A (2013) RAVAGE: post-silicon validation of mixed signal systems using genetic stimulus evolution and model tuning. In: 2013 IEEE 31st VLSI Test symposium (VTS), pp 1–6
69. Jin Y, Maliuk D, Makris Y (2012) Post-deployment trust evaluation in wireless cryptographic ICs. In: 2012 Design, automation test in europe conference exhibition (DATE), pp 965–970
70. Wang YT, Chen DJ, Geiger RL (2013) Effectiveness of circuit-level continuation methods for Trojan state elimination verification. In: 2013 IEEE 56th International midwest symposium on circuits and systems (MWSCAS), pp 1043–1046
71. Li Y, Chen D (2014) Efficient analog verification against Trojan states using divide and contraction method. In: 2014 IEEE International symposium on circuits and systems (ISCAS), pp 281–284
72. Liu S, Geiger RL, Chen D (2014) A graphical method for identifying positive feedback loops automatically in self-biasing circuit for determining the uniqueness of operating points. In: NAECON 2014 - IEEE National aerospace and electronics conference, pp 384–390
73. Liu Z, Li Y, Duan Y, Geiger RL, Chen D (2014) Identification and break of positive feedback loops in Trojan states vulnerable circuits. In: 2014 IEEE International symposium on circuits and systems (ISCAS), pp 289–292