# Chapter 6
# Hardware Trojans and Piracy of PCBs

**Anirudh Iyengar and Swaroop Ghosh**

## 6.1 Introduction

Authenticity and security concerns due to hardware Trojans and counterfeiting at the integrated circuit (IC) level have been studied extensively in recent times [1]. However, vulnerability with respect to hardware Trojans and cloning at higher levels of system abstraction, e.g., at printed circuit board (PCB) level, has not been well reported. PCBs are extensively used in every electronic system to enable electrical interconnections between components and for mechanical support. The emerging business model of PCB design and fabrication that favors extensive outsourcing and integration of untrusted components/entities in the PCB life cycle to lower manufacturing cost makes both malicious modification and cloning of PCBs highly feasible [2]. Closer inspection of several common electronic products (e.g., mobile devices and wearables) and their PCB manufacturers reveals that different parts of PCB designs (e.g., schematic and layout) are often carried out in different physical locations by different parties. Therefore the PCBs are greatly exposed to reverse engineering, counterfeiting, overproduction, Trojan insertion, and recycling. Unlike integrated circuits (ICs), where researchers have analyzed the various flavors of hardware security primitives [3, 4], PCB security primitives are still evolving. Previous studies have covered security of PCBs against piracy and various post-fabrication tampering attacks. JTAG (Joint Test Access Group) and other field programmability features, e.g., probe pins, unused sockets, and USB, have been extensively exploited by hackers to gain access to internal features of the designs

A. Iyengar (✉) • S. Ghosh
Department of Electrical engineering and computer science, Pennsylvania State University, Pennsylvania, PA 16802, USA
e-mail: asi7@psu.edu; szg212@engr.psu.edu



S. Bhunia, M.M. Tehranipoor (eds.), *The Hardware Trojan War*,
https://doi.org/10.1007/978-3-319-68511-3_6

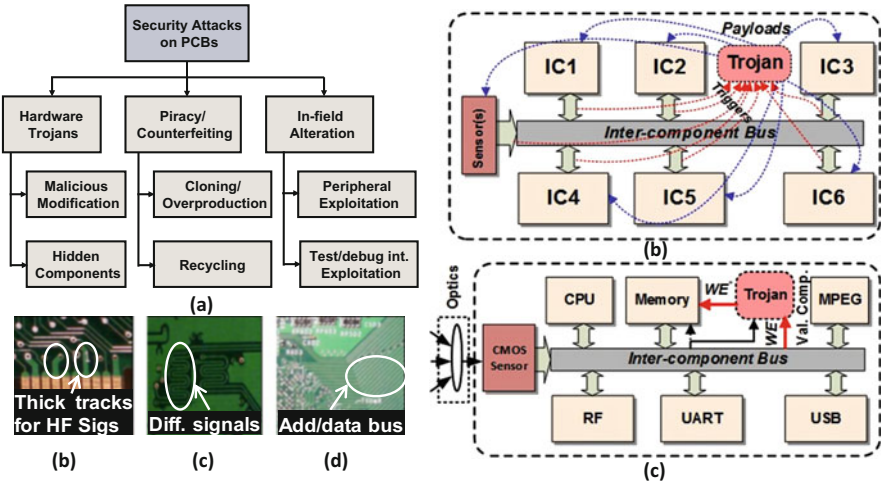


**Fig. 6.1** (**a**) Taxonomy of various attacks on PCB; (**b**) general model of PCB-level hardware Trojan; (**c**) a specific example of Trojan affecting the external memory access in PCB. Vulnerabilities in PCB design with respect to Trojan attack: (**d**) thicker traces for high-frequency signals, (**e**) pair of signals for differential signaling, and (**f**) group of traces indicating bus [12]

[5] as well as snooping of secret key, collection of test responses, and manipulating JTAG test pins [6]. One instance demonstrated that Xbox can be hacked by disabling the digital rights management (DRM) policy using JTAG [5–7]. We note that modern PCBs are becoming increasingly vulnerable to malicious modification of PCBs during design or fabrication in untrusted design or fabrication facilities unlike the widely reported infield tampering attacks [3–9], such a vulnerability creates a new class of threat for PCBs.

This reliance to third-party manufacturing facilities makes the PCB fabrication process untrustworthy and, hence, vulnerable to malicious modifications, i.e., Trojan insertion and piracy, i.e., counterfeiting. Furthermore, an adversary can be present inside the design house, and the PCB design can be tampered with Trojans. Figure 6.1a shows broad classes of attacks on PCB including possible Trojan attacks.

In this chapter, we provide an overview of the various PCB security challenges [10]. We describe several instances of PCB attacks and review some of the more recent mitigation techniques/countermeasures. The chapter is organized as follows: The security challenges are introduced in Sect. 6.2.1. The attack instances of hard to detect Trojans are described in Sect. 6.2.2. Potential countermeasures are detailed in Sect. 6.2.3. Section 6.3.1 describes the authentication challenges, while Sect. 6.3.2 illustrates PUF structures. Finally, Sect. 6.3.3 provides a quantitative and qualitative analysis of the PUFs.

## 6.2 PCB Security Challenges, Attacks, and Countermeasures

### *6.2.1 Security Challenges*

#### 6.2.1.1 Security Analysis

An attacker can exploit the vulnerabilities, design/test features, and test hooks that are available on the board. Some common PCB features that can be exploited by an adversary for understanding a design intent and efficiently mounting a Trojan attack with minimal design modification are as follows:

(a) *JTAG interface* – JTAG is an industry standard to enable board-level test and debug. It can be exploited by a hacker to get a clue about the hidden test features or hidden control to access the data and address bus within the chip [5–7]. For example, hackers can deduce information about the length and properties of the instruction register through JTAG by trial and error. Next, a particular instruction can be executed to gain permission to tamper/feed internal data bus. JTAG can also be used to reverse engineer (RE) the board design by deducing the connectivity between components and executing external connectivity instructions. Aside from this, JTAG can be exploited too.

(b) *Test pins or probe pads* – Typical ICs contain several probe pads and test pins to observe/control important signals for test/debug purposes. A hacker can tap these pins and monitor the interesting signals to gain critical information about the functionality of the design or feed malicious data into the design. Test pins can also be used for RE where a test input can trigger certain data and address and control signals that can help identify the board functionality.

(c) *Infield alteration* via *ModChips* – This involves alterations caused by mounting integrated circuits, soldering wires, rerouting paths to avoid or substitute existing blocks, adding or replacing components, and exploiting traces, ports, or test interfaces in ingenuous manners [7, 11]. ModChips are one such class of devices that alter the functionality or disable restrictions within a system, such as computer or game console [12]. For instance, Xbox ModChips can modify or disable the built-in restrictions integrated in Xbox consoles, allowing to play pirated games in the tampered consoles.

(d) *Vulnerabilities in PCB design* – Figure 6.1d–f illustrates several additional vulnerabilities as described below:

  (i) *Distinct properties of special signals*: The thickness of clock and data bus provides clues to the hackers about the functionalities of these pins. Similarly, pins tied with identical pull-up/pull-down resistors indicate that they belong to a bus.

  (ii) *Remnant signatures from test/debug*: When pins (that are used for test/debug) are accessed through ports, the remnant of soldering provides clue to a hacker about the functionality of these pins. Similarly, an empty socket can be used for hacking purposes.

**a**

| Security Vulnerability in PCB | Possible Exploitation for Trojan Attacks |
|---|---|
| JTAG | Hacking of scan chain / data bus for illegal access to memory / logic |
| RS232, USB, Firewire, Ethernet | Hacking of internal memory of an IC, leaking of secret data |
| Test Pins | Access to internal scan chain to leak data from ICs |
| Unused Pins, Multiple Layers, Hidden Vias | Alteration of connections using internal layers / hidden vias |

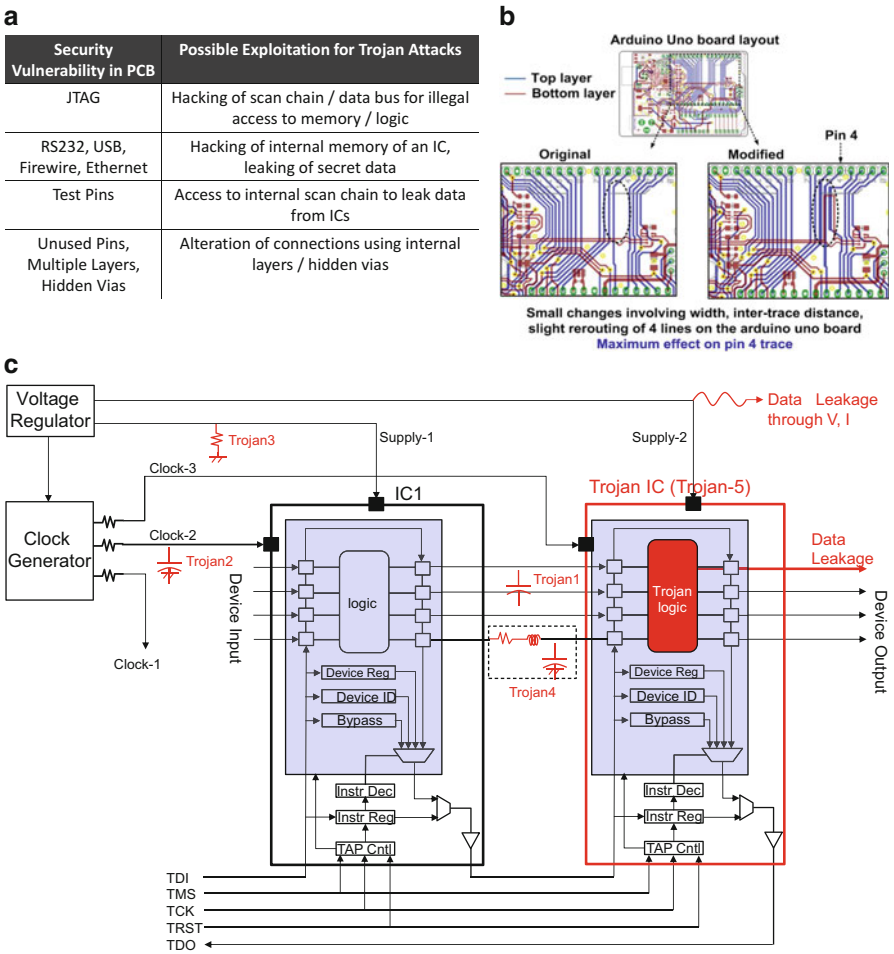


**Fig. 6.2** (**a**) Vulnerability at PCB level with respect to Trojan attacks; (**b**) minor modifications in Arduino Uno board layout to insert Trojans without addition of any new component; and (**c**) examples of hardware Trojan insertion in a PCB component [10]

(iii) *Miscellaneous hints*: Figure 6.2a lists some additional vulnerabilities. Apart from the above component-level hooks, a PCB design itself provides lots of information to an adversary in fabrication house that can facilitate powerful Trojan attacks.

#### 6.2.1.2 Attack Models

Trojan attacks in PCB can be divided into two broad classes, as described below:

1. *Case I*: The board design is trusted. In this model, the attack is mounted in the PCB fabrication house. It is expected that the attacker would change the design in a way that evades post-manufacturing test but causes functional deviations under certain rare conditions, which are unlikely to be triggered during test.
2. *Case II*: The board design is not trusted (e.g., outsourced). In this model, the attacker is assumed to be present in the board design or fabrication house. Only the functional and parametric specifications of the board are trusted. The attacker has higher flexibility of maliciously altering the design and/or choosing fake or untrustworthy (and potentially malicious) components. Again, an attacker would try to hide the modifications to avoid detection during functional and parametric testing process.

Note that in both cases, there are two possible objectives of the attacker: (1) malfunction and/or (2) information leakage. Next, the possible Trojan attacks of different forms in a PCB are described.

(a) *Signal trace modifications in the inner PCB layers*: For boards with fewer levels where hiding an extra component is difficult, an attacker can change the resistance, capacitance, or inductance of the signal traces (self, mutual). For example, signal trace in an internal layer can be made thinner to increase the resistance such that it fails during long hour of operation due to heating. Similarly, the metal coupling capacitance between two traces including traces in the supply planes can be increased (by changing trace dimensions, inter-trace distance via slight rerouting, and selective dielectric property modification) to trigger coupling-induced voltage and delay failures in one of the lines. Leakage resistance paths can also be incorporated in an internal layer trace for intentional voltage degradation. Impedance mismatch between interconnected traces can be introduced to cause malfunction in certain scenarios.

Modification in an example trace-4 scenario, causing malicious effects on circuit parameters (coupled voltage, delay failures, and voltage degradation), is illustrated in a commercial Arduino Uno board layout in Fig. 6.2b. It involves changing the thickness and inter-trace distances by 2X and rerouting of single trace. Even in a small two-layer board design like the Uno, these changes are minimal and difficult to detect during the test but can cause undesired functional behavior under certain scenarios. In complex PCB designs with more than four layers, these changes would be confined within a small area of an internal layer. Hence, the chances of detection with optical or X-ray-based imaging are extremely low. Functional testing is typically not exhaustive, and hence these can easily bypass detection. However, in certain rare conditions in field, their effect on circuit parameters can be significant causing system failures.

(b) *Hidden components*: For boards with more than two layers, an adversary can insert extra components in an internal layer to either leak information or conditionally cause malfunctions. Replacing a legitimate IC with Trojan-infected IC is another possibility (Fig. 6.2c). The tampered IC would be functionally equivalent to the legal IC; however, it may be equipped with capabilities to leak secret information. The leakage can be direct (through unused pins) or indirect (modulating supply voltage or current). Figure 6.1a summarizes different categories of PCB attacks.

## *6.2.2 Attack Instances*

### 6.2.2.1 Design House Is Trusted

This scenario arises when the PCB is designed by a trusted designer and outsourced for fabrication. During the manufacturing process, malicious modifications can be intelligently inserted by an adversary, such that the final design structurally matches the original one (no additional components, logic, traces) but produces undesired functionality under certain conditions. The small alterations can be confined in the internal layers of a multilayer PCB. Hence, chances of detection with visual inspection, optical imaging, and X-ray-based imaging techniques are low. Besides, exhaustive functional testing is typically impossible with large number of test nodes. Therefore, the malicious functions are very likely not triggered during the in-circuit and boundary scan-based functional testing [13]. Usually modifications can be made in the existing traces to increase the mutual coupling capacitance, characteristic impedance, or loop inductance by changes in internal layer routing and small leakage path insertion. Additional components with ultra-low area and power requirements can also be inserted in the internal layers. Two Trojan examples are presented in this class. The first case considers a multilayer PCB (10 cm length) with possible application in a high-speed communication and video streaming systems. It has a common scenario of two high-frequency (HF) PCB traces in an internal layer running parallel to each other. Typically, HF traces are routed in the internal layer shielded by power and ground planes to avoid interference (Fig. 6.3a). However, it significantly complicates the internal layer testing and debug procedure and provides an opportunity to the attacker. The dimensions of the traces are designed optimally to carry normal HF signals, i.e., 1 oz. copper trace with width and thickness of 6 mils and 1.4 mils, respectively [14]. The dielectric is FR-4 with a relative permittivity of 4.5. The inter-trace distance is chosen to be 30–40 mils to avoid the negative effects of mutual inductive and capacitive coupling. These HF traces are modeled by lumped parametric form [14]. Functional simulation shows a maximum coupled near- and far-end voltage of $\sim$300 mV p-p on one of the traces, with the other trace swept with pulse voltages of 3 V p-p at 10–500 MHz with a 50% duty cycle. The maximum propagation delay for the pulse across the active trace is $\sim$0.4 ns.

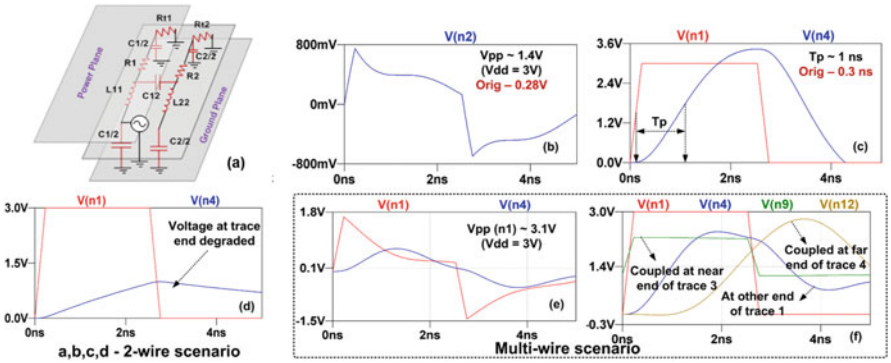


**Fig. 6.3** Impact of Trojans in a PCB inserted by selective trace/s property modification, without addition of any new component (design house trusted scenario): (**a**) lumped trace-2 PCB model with associated capacitance, inductance, and resistance; (**b**) trace-2 near- and far-end voltages and (**c**) propagation delay in trace-1 (n1 and n4 nodes) at 220 MHz and 3 V p-p input; (**d**) effect on trace-1 far-end voltage, on insertion of a leakage resistance path from trace-1 to ground; (**e**) and (**f**) show the effect of change in trace properties in a four-wire scenario. Coupled voltages in near and far end of victim trace, when all aggressors are switching in phase at 220 MHz and 3 V peak-to-peak (p-p), are illustrated in (**e**), and voltage profile at near end (n9) of trace-3 and far end (n12) of trace-4 is shown in (**f**) [10]

With the simulation setup described above, we observe the effects of various trace level modifications during fabrication. The inter-trace distance in the internal layers is reduced by 2X, widths of both wires are increased by 2X, and the thickness is increased by 1.5X. These are minimal changes in a small target region of an internal layer, rendering them mostly undetectable during structural testing. The dielectric permittivity of the insulator between the traces is increased to 5.5 in order to model moisture retention in certain insulating areas, impurity addition to epoxy base [15], and, hence, the aging effect. Accelerated aging tests have a low probability of detecting this as the permittivity is selectively altered by an adversary in a small area. However, the effect of these changes on associated circuit parameters can be significant.

At 220 MHz, the near-end peak-to-peak voltage in trace-2 is ∼1.4 V for an input pulse voltage of 3 V p-p in trace-1 (Fig. 6.3b). This is an extraneous interference and may cause unexpected behavior in terms of erroneous circuit activation or feedback. The propagation delay increases by 2X, beyond 1 ns (Fig. 6.3c) which can induce functional failures for higher switching frequencies and greater trace lengths. From an attacker's perspective, inserting a small leakage path (2X the trace resistances) to ground can drain away the signal, resulting in a degraded, distorted waveform at the far end of trace-1 (Fig. 6.3d) and hence malfunction in the connecting circuits. This can easily evade detection by conventional PCB testing which is not exhaustive due to prohibitive cost and time to market.

The effect of coupling is more prominent when multiple HF traces, over different planes, are intentionally routed intelligently to increase mutual coupling. This can be

achieved by (a) bringing the in-plane neighboring traces closer and (b) increasing widths and thicknesses of the lines. These selective minute alterations are highly likely to pass structural and functional testing. However, the effect of these changes on the circuit performance could be significant as shown in Fig. 6.3e–f. The coupled voltages at the near and far end of victim trace-1 are 3.1 V p-p and 1.3 V p-p, respectively (Fig. 6.3e), with in-phase rising/falling transition on the adjacent three traces (one in-plane, one above, and one below). This is 34X greater than the case when active traces are switching in opposite directions. This interference would certainly result in failures in terms of erroneous activation, feedback, and performance. The voltage profile at the far end of trace-1 with the others inactive shows some distortion and an average propagation delay of 1 ns (Fig. 6.3f). Higher number of neighboring traces and greater trace lengths significantly affect the propagation delay and cause delay failures at high switching speeds. Extraneous coupled voltages in trace-3 and trace-4 are illustrated in Fig. 6.3f as well. It can be noted from the above results that detecting these Trojans is extremely hard since it is sensitized under very rare specific conditions. In the multi-wire scenario, the degraded performance is prominent only in two out of eight possible combinations of transition polarity (i.e., all rising/falling pulses) in the three neighboring traces. The frequency of operation and the input vector patterns serve as two example conditional triggers for these Trojans, inserted by selective trace property and routing alterations during PCB fabrication.

#### 6.2.2.2 Design House Is Untrusted

In this attack model, both PCB design and fabrication are done in untrusted facilities, thus increasing the possibility of Trojan attacks. The board specifications generated by the system designer are trusted. Post-manufacturing testing is done by the system designer to ensure the board performance and functionality. Hence, along with the possibilities of trace level alterations, an attacker can also leverage the opportunity to modify the design structurally and/or insert additional components that would be activated upon certain trigger conditions. The design alterations would be hidden intelligently (e.g., physically or by rare input conditions) to evade detection during post-fabrication structural and functional testing. A simple example of this attack model is illustrated in Fig. 6.4, where a fan controller adjusts the speed of a 12 V DC brushless fan based on the input received from a temperature sensor. The sensor provides 0–5 V (depending on the current temperature) which is digitized by an ADC and sent to a microcontroller that controls the speed of the fan through linear regulation of the fan input voltage.

With minor structural modification, an attacker can maliciously tamper with the functionality of the circuit (Fig. 6.4a). In this case, the Trojan prevents the microcontroller from obtaining an accurate temperature. It includes a resistance, a capacitor, and a PMOS transistor. The capacitor is charged using the output from a voltage regulator (LM317) connected to the fan. The time needed to activate the Trojan (i.e., the trigger condition) can be adjusted by manipulating the resistance and

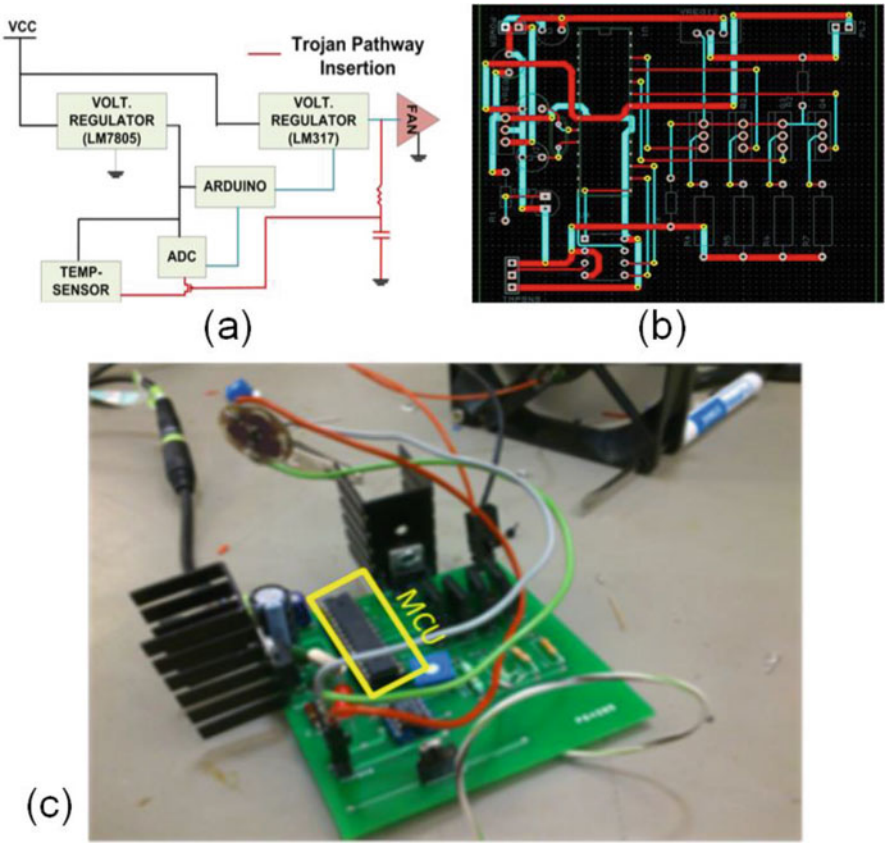


**Fig. 6.4** (**a**) Fan controller circuit with a Trojan insertion; (**b**) a two-layer PCB layout of the original circuit; and (**c**) a fabricated PCB board which demonstrates triggering and payload of the Trojan [10]

capacitance values. The trigger deactivates the PMOS transistor inserted between the temperature sensor and the ADC, effectively disabling the connection. Hence, the microcontroller receives a null input that is interpreted as a very low temperature, and the fan speed is reduced significantly. With a large value of time constant, this design alteration has a high probability of evading functional testing. A two-layer PCB schematic of the fan controller (prefabrication) is shown in Fig. 6.4b. A fabricated PCB board to demonstrate the triggering and payload of the Trojan is shown in Fig. 6.4c.

From the above discussion, it is obvious that achieving these minor structural modifications in such a scenario is easy due to outsourcing of both design and fabrication. Since system integrator only possesses information about the major PCB components (constituent ICs) and functional specifications, such small alternations can go undetected. From the attacker's perspective, a multilayered PCB is more

attractive because it provides increased opportunities to hide the design changes. In addition to the structural changes, an adversary in the foundry can perform layout modifications to deliberately insert trace level Trojans, which are difficult to identify by functional tests.

### *6.2.3 Possible Countermeasures*

#### 6.2.3.1 Hardware Trojan Detection in PCB

In [10] a noninvasive RE and multiparameter side-channel analysis to detect the embedded Trojans is proposed. First, the Trojans are categorized by their nature, e.g., Trojans that induce (a) parametric failures, such as unacceptable delay and leakage (Trpar), (b) large static power (Trpwr), and (c) functional failures (Trfn). Trojans in each category are treated differently for detection. Next, a criticality analysis is performed to isolate the vulnerable nodes. This step is conducted to identify the critical signals from design specification, e.g., clock, control signals, data, and address bus. The PCB layout information is captured in the analysis to identify the potential Trojans (i.e., the longest trace that runs in parallel with the victim signal). For analysis we assume that (a) an intended PCB design is available to the validation engineer, (b) a single Trojan is inserted at a time, (c) a Trojan injection is limited to neighboring traces, and (d) the tampering does not involve change in the signal routing.

Test pattern generation for Trojan detection can leverage on the principles of conventional testing. The PCB layout and criticality analysis generate a list of possible triggers/payloads and their locations. Test patterns are generated to sensitize the trigger conditions of each Trojan and observe its effect. The process continues till all the Trojans in the list are exhausted. Side-channel analysis such as delay, frequency, static leakage, and dynamic current can also be administered to sensitize Trojans of other types. Side-channel analysis, however, would require a set of golden PCBs. The Trojan coverage and the test patterns are output of the proposed methodology (Fig. 6.5a). The test patterns obtained above are applied to both extracted parasitic model and actual PCB, and their responses are compared to detect Trojans. Figure 6.5b illustrates this methodology for capacitive Trojans through an example where net n3 is identified as the target signal from node criticality analysis. Therefore, the Trojan list would contain {c1, c5, c6}. For this example, test pattern will target to toggle nets n1, n3, and n5 in association with n3 to sensitize the Trojans for detection. Note that c2 is excluded from the list due to shorter track segment of n2 in parallel with n3.

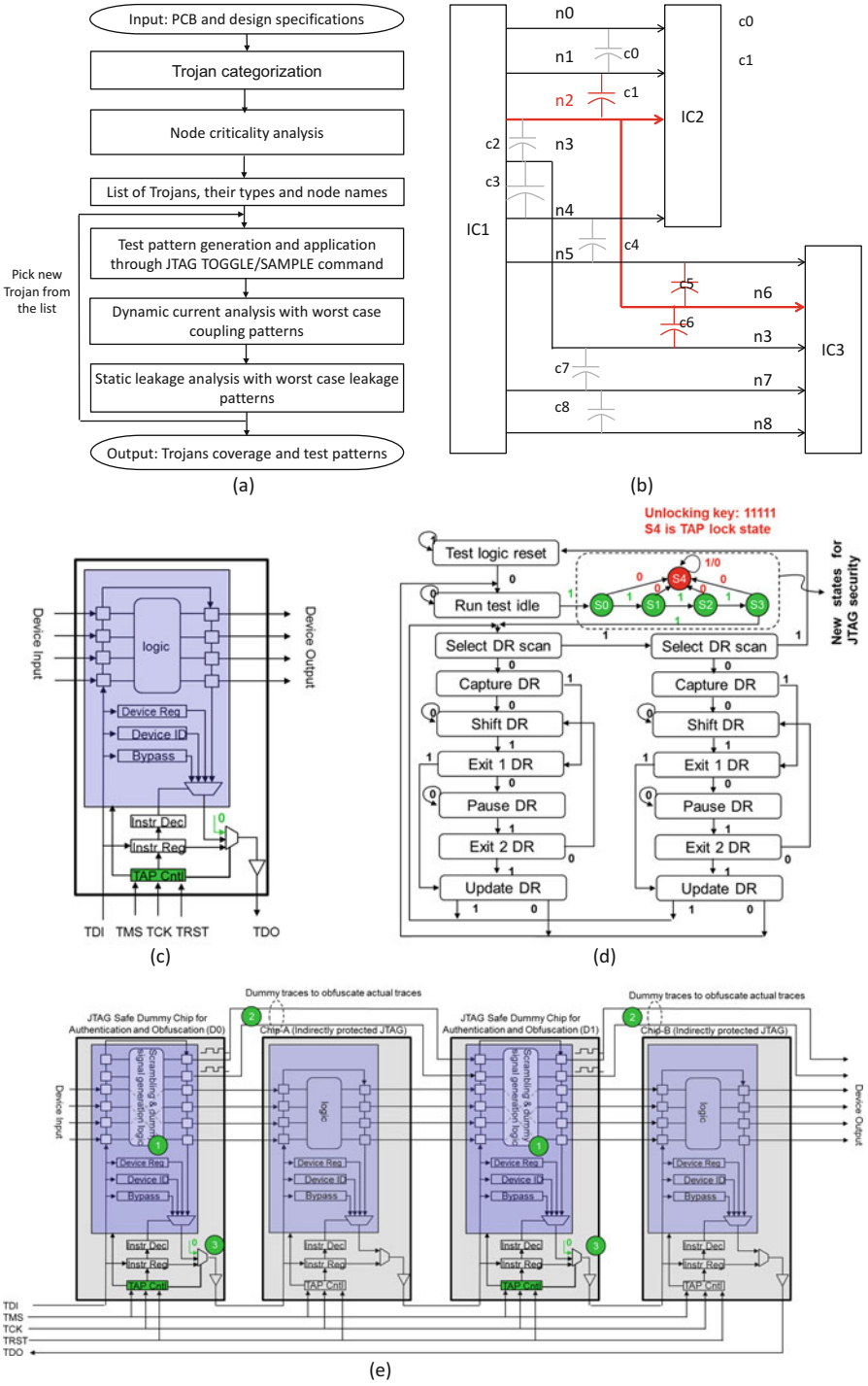


**Fig. 6.5** (**a**) Flowchart of the Trojan detection methodology [10]; (**b**) example illustrating the capacitive Trojan detection; (**c**) modified tamperproof JTAG interface incorporating the TAP controller; (**d**) TAP controller state diagram; and (**e**) incorporation of dummy ICs to obfuscate the PCB interconnects

#### 6.2.3.2 Preventive Countermeasures Through Hardening

The following proactive techniques are proposed in [10] to protect against Trojan attacks in PCBs:

1. *Secure interfaces*: Conventional JTAG cannot prevent unauthorized access, and therefore it can be exposed for tampering. The security features inside JTAG are updated so that the access to instruction and data registers is restricted until a code/password is fed to unlock the TAP controller. Figure 6.5c shows the JTAG structure containing TAP controller that provides access to the instruction and data register (device registers, ID register, and bypass register) based on TMS and TCK. The modified TAP controller (Fig. 6.5d) includes newly added states (S0–S3) that look for a certain security key. In order to allow legitimate access (for installing upgrades and patches), the secure JTAG can be unlocked by feeding the correct keyword (0011111 in this case). However, in the event of wrong keyword, the controller will go to a lock state (S4) where it will disconnect the TDI and TDO by feeding a fixed value to TDO. Note that once the TAP goes to the lock state, it cannot be reset back to factory state preventing the possibility of a trial-and-error method by the hacker.
2. *Secure PCB*: Conventionally designed PCB traces can be reverse engineered to discover the board design. An approach is proposed in [10] to address this challenge through interconnect obfuscation. Figure 6.5e shows one possible approach to obfuscate the interconnects by introducing dummy ICs that serves three purposes:
   (a) It scrambles the traces based on a scrambling function implemented in the dummy logic. The dummy device is RE resistant due to the presence of secure JTAG that prevents access to internal design without proper authentication.
   (b) It provides dummy outputs that are mixed with real traces to confuse the hacker. The dummy traces are driven by random logic and counters to obfuscate the data, address, and clock signals. Furthermore, the dummy traces are drawn in the same way as the real data and clock signals to obfuscate the real signals.
   (c) It implements secure JTAG; therefore the access to real chips is also secured even if they implement unsecured JTAG. In order to RE the real chips, the hacker needs to unlock the JTAG of two dummy chips (D0 and D1) each of them may have different security keywords. RE through JTAG could be deterred further by incorporating the security states in the TAP controller of the real chips as well.

#### 6.2.3.3 Tamper Detection and Prevention

In this approach, a real-time system monitoring is enforced in order to prevent tampering [11]. A critical trace is identified and is compared with an expected value.

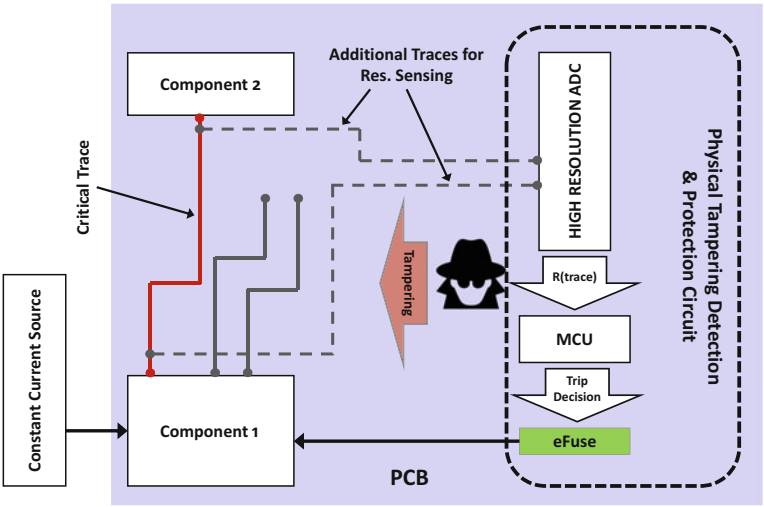


**Fig. 6.6** A functional block diagram of the prototype tamper detection and prevention circuit on a PCB [11]

Any deviation from this value can be identified by which the attack can be prevented. Figure 6.6 describes the general methodology, where the components of interest are identified along with their critical trace. During an attack, the resistance of the critical trace will vary, which is correspondingly identified by the tamper detection circuit. This is then relayed to an eFuse to shut down the device.

## 6.3 PCB Authentication Challenges and Prospective Solutions

Aside from the Trojan attacks, PCBs are highly susceptible to cloning. This is further exacerbated by the high distributive manufacture process. To solve similar problem, ICs typically employ a physically unclonable function (PUF) [16], which exploits device specific parameters toward generating a unique and authentic signature. Such features however are still evolving in PCBs. One such work is the *BoardPUF* [17], which employs the capacitance difference of an embedded comb-like structure to generate response for a given challenge during authentication. Figure 6.6 illustrates the architecture of the BoardPUF, with the variation source to be the capacitor which is composed of a set of well-designed comb-like pattern which is placed between layers of PCB, to reflect the variations observed during PCB manufacture. A counter is used to record the signals by the sensing circuits for a given time interval. This is then compared with counts from different compare units specified by the compare pairs through which the final ID is generated.

Although attractive, most of the authentication process is done via the on-board chip, which can be corrupted and can lead to denial of service.

Another PCB-based PUF authentication methodology, proposed in [18], exploits the impedance of PCB traces toward generating a unique signature at no area overhead. The trace impedance being unique to each PCB acts as a good source of authentication. However, one of the major drawbacks of this technique is the sheer lack of eligible traces that can be directly probed. As most of the PCB interconnections are in the internal layers, gaining access to a significant set of interconnects at the top/bottom layer is difficult. This limits the number of responses that can be obtained from the PCBs. Aside from this, work done by Andrew et al. [7], utilizes the Boundry Scan Chain Architecture (BSA) design on the JTAG, to create a unique signature from each PCB for authentication. The technique exploits the inherent delay of the BSA for authentication. Due to manufacture-induced process variations, the delay value of the BSA also varies correspondingly. Therefore, the resultant delay is unique to each device. By correctly determining the delay, one can distinguish one device's delay with another. Thus, allowing us to deterministically authenticate the device at hand. In an effort to realize a "strong-PUF," Anirudh et al. [19] proposed a unique PCB-based PUF design that captures a high degree of process variation and also facilitates a large number of challenge-based responses. Before dwelling into the design, we first need to understand the various authentication challenges the PCBs face.

## *6.3.1 PCB Variations and Authentication Challenges*

### 6.3.1.1 Sources of Variations

PCB manufacturing process can introduce various physical, electrical, and chemical variations. These variations are broadly categorized as follows [19]:

(a) *Variations in trace physical dimensions:* This variation alters the electrical properties of the trace such as resistance, inductance, and capacitance causing a deviation from the expected behavior.
(b) *Variations in* via *dimensions:* This leads to an overall variation of via impedance. Larger the number of vias for a single signal, greater is the impedance variation.
(c) *Density variations:* Variations in deposition density also leads to impedance variations. Cavities (mouse bites) are observed in long traces, causing a shift in the electrical characteristic of the trace [20].
(d) *Alignment between layers:* Misalignment of masks during manufacturing leads to variation in trace deposition.
(e) *Layer lamination:* Unevenly thick layers can result in some vias being taller than the others and can also impact embedded capacitance, which too impacts its intrinsic impedance.

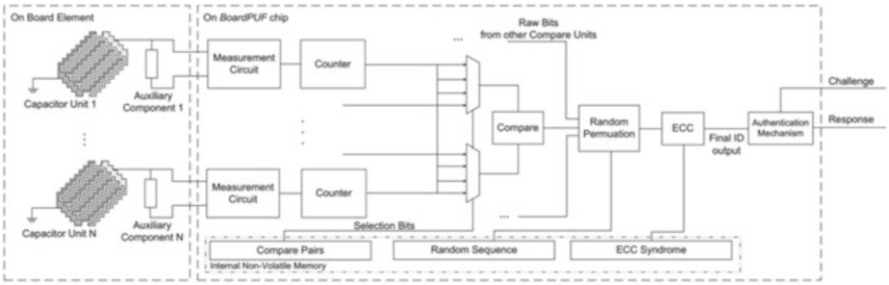


**Fig. 6.7** BoardPUF architecture [17]

The above variations sources affect each PCB differently, making them perfect candidates for PCB authentication (Fig. 6.7).

#### 6.3.1.2 Qualitative Analysis of Authentication Issues and Metrics

One of the primary issues with PCB authentication using PUF is limited number of challenges. Each PUF structure such as embedded comb [17] and PCB trace [18] acts as a single challenge and provides single response. This is unlike IC PUF where linear and exponential number of Challenges Response Pairs (CRPs) can be generated. Generating exponential CRPs at low area overhead is a challenge. Designing passive structures to convert the PCB variability (as discussed in Section II.A) into a response is another key issue.

A key metric used to determine the quality of the PUF is the Hamming Distance (HD). HD is the amount of variation one PUF signature is with another. For a good (strong) PUF, the HD should be ideally 50%. The simple HD can be divided into inter-die HD and intra-die HD. Where the inter-die HD is the HD between two PUF responses of different devices, while the intra-die HD is the variation in the PUF signature of one device w.r.t. environmental changes such as temperature, humidity etc.

The concept of inter-die Hamming Distance (HD) metric can be extended to obtain inter-PCB HD. The objective of this metric is to ensure sufficient difference between responses of two PCBs for the same challenge (i.e., PUF structure in this case). The concept of intra-HD used in IC authentication may not be readily applicable to PCB though. This is due to the fact that temperature and voltage during authentication depends on usage scenario. When the external bare PCB is authenticated by the vendor, they can follow the exact voltage and temperature conditions specified by the PCB manufacturer during authentication. Therefore, intra-PCB HD will be 0%. However, when the PCB is assembled and deployed in product it could be interrogated by the secure facility such as bank. Under this circumstance the ambient temperature could be different. The voltage could still be the same; however, the environmental moisture could be different. Therefore, the

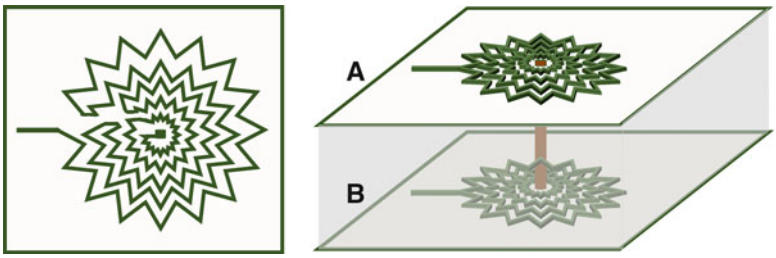


**Fig. 6.8** PUF features: coil (**a**) *top view* and (**b**) structure comprising of symmetric zigzag coils separated by a dielectric. The notches capture edge rounding variations in resistance and inductance whereas two coils in two layers capture the capacitance variation due to misalignment [20]

intra-PCB HD should consider temperature and moisture variation to determine the stability.

### *6.3.2 Prospective PUF Structures*

A passive structure has been proposed [19] that can capture various sources of variations to provide a unique device signature [20]. Figure 6.8 illustrates a coil-type structure which is designed using Allegro [21] PCB editor. Compared to a typical straight coil, this structure exhibits additional resistance (wire resistance), capacitance (enhanced due to the comb-shaped multilayer design) and inductance (enhanced due to the coil shape) variation due to the high number of notches. Therefore, this structure is suitable for capturing the many sources of manufacturing process variations including edge rounding, density, and alignment variation.

#### 6.3.2.1 Star-Coil PUF

This PUF works by exploiting the resonance frequency (RF) of the star-coil for authentication. RF being unique to each coil (due to unique set of process variation) acts as a good source of authentication. The star-coil is excited by a voltage source, whose frequency is swept from a given minima to maxima. The frequency at which the current through the coil is the highest, i.e., impedance is the least, is its resonance frequency. The resonant frequency for an RLC circuit is given by:

$$f_{\text{res}} = {}^{1}\Big/_{2.\pi.\sqrt{\text{L.C}}} \tag{6.1}$$

where "$f_{res}$" is the resonance frequency in Hz, "L" is the inductance in Henry, and "C" is the capacitance in Farads. Due to the inverse relationship between impedance (ignoring resistance) and resonance frequency, a small change in the impedance

results in a large change in the resonance frequency. In order to understand the impact of process variation on the resistance (R), inductance (L), and capacitance (C) of the coil, a 10% introduced variation (assuming it to be 3σ variation) on the trace length, width and dielectric thickness. We know from [19] that a linear relationship of R, L, and C with respect to the trace length, width, and thickness persists. This observation is used in determining the mean and standard deviation of R, L, and C due to each variation.

$$\Delta 1 = \text{guassian distribution of trace length}$$

$$\Delta 2 = \text{guassian distribution of trace width}$$

$$\Delta 3 = \text{guassian distribution of dielectric width}$$

$$\begin{aligned}\text{Total Inductance (L)} = {} & \text{Inductance}\,(\Delta_1) + \text{Inductance}\,(\Delta_2) \\ & + \text{Inductance}\ (\Delta_3) + \mu_{\mathrm{L}}. \end{aligned} \tag{6.2}$$

$$\begin{aligned}\text{Total Capacitance (C)} = {} & \text{Capacitance}\,(\Delta_1) + \text{Capacitance}\,(\Delta_2) \\ & + \text{Capacitance}\,(\Delta_3) + \mu_{\mathrm{C}}. \end{aligned} \tag{6.3}$$

$$\begin{aligned}\text{Total Resistance (R)} = {} & \text{Resistance}\,(\Delta_1) + \text{Resistance}\,(\Delta_2) \\ & + \text{Resistance}\,(\Delta_3) + \mu_{\mathrm{R}}. \end{aligned} \tag{6.4}$$

where $\mu_{\mathrm{L}}$, $\mu_{\mathrm{C}}$, and $\mu_{\mathrm{R}}$ are mean values of inductance, capacitance, and resistance, respectively.

By combining the effects of trace length, width, and dielectric thickness on the overall R, L, and C (using 2–4), a cumulative mean and standard deviation of the star-coil PUF is obtained. A 10000-point Monte Carlo analysis performed on the trace length, width, and dielectric thickness reveals the corresponding resonant frequency distribution. The plot is as shown in Fig. 6.9. A spread of 10 MHz in the resonant frequency is observed.

This design can be extended to incorporate more variations by using multiple such coils connected together in a serial or parallel fashion (illustrated in Fig. 6.10a–d). This allows us to exploit the use of multiple layers (thickness variations, lead to impedance variations), which further adds to the variations that the circuit experiences. Measuring the resonance frequency of this stack will provide a signature truly unique to the PCB.

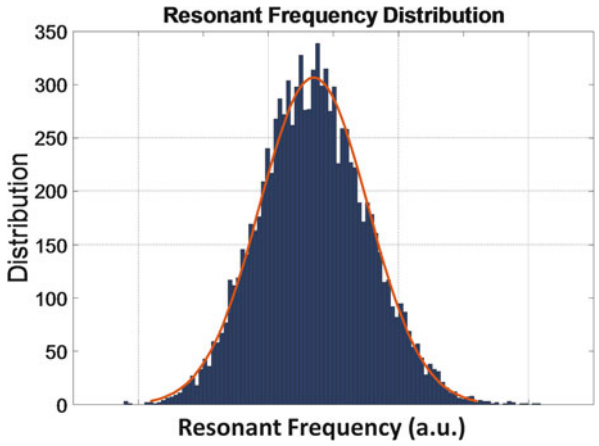


**Fig. 6.9** Resonance frequency distribution [19]

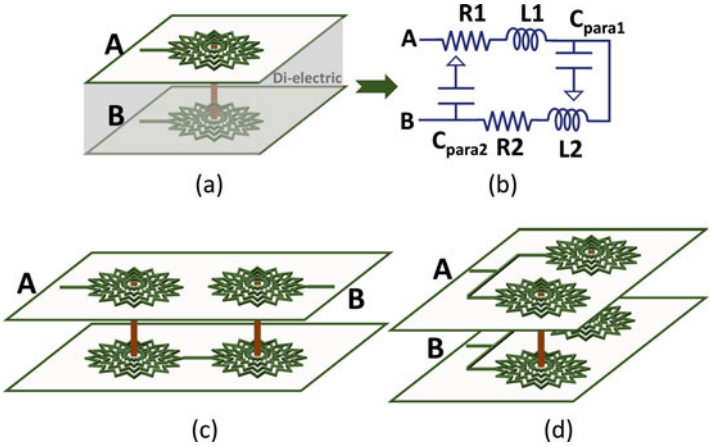


**Fig. 6.10** Star-coil structure: (**a**) base configuration, (**b**) equivalent RLC circuit, (**c**) series connected coils, and (**d**) parallel coil combination [19]

### 6.3.2.2 Arbiter-Coil PUF

One major limitation of the coil PUF is that, it has only one possible outcome (one signature) for authentication. This does not adequately provide us linear or exponential number of responses for reliable authentication. In order to improve the CRPs a passive arbiter-PUF is proposed [17] where several stages of star-coils are connected in various possible combinations to form a path through external jumpers (manually connected during authentication) (as seen in Fig. 6.11). By varying the jumper connection in accordance to a certain "challenge", a corresponding response unique to the path is obtained. The process can be repeated for different challenges (paths) to get additional resonance frequency values. By comparing all these values to the values stored in the database, a PCB can be authenticated with a high degree

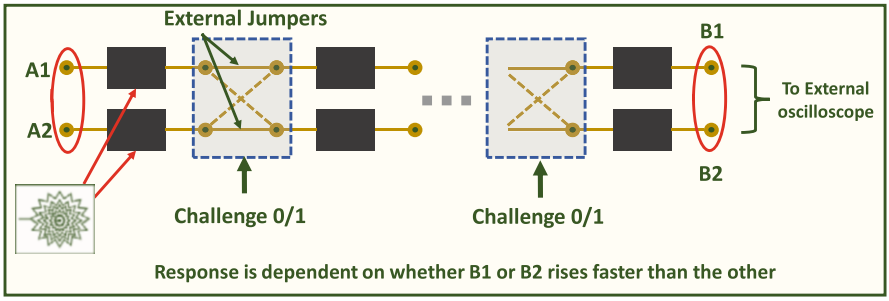


**Fig. 6.11** Arbiter design-based PCB PUF [19]

of reliability. This PUF is considered as a strong-PUF due to its exponential increase in CRPs with the increase in the number of rows and/or stages of coil PUFs. Note that other types of passive structures (such as straight traces, comb traces) can also be used in the individual PUF stage instead of the star-coil.

Aside from the abovementioned resonant frequency determination approach, the arbiter-coil PUF can be used to measure the delay difference between the two paths (with cascaded stages). As the rise/fall of the signal is directly proportional to the capacitance and inductance of each individual coil, the cumulative effect will provide an alternative means of authentication. To show proof of concept, Anirudh et al. [19] show a 1 stage, 128 copy arbiter-coil-based delay PUF. A Gaussian distribution on the R, L, and C obtained from allegro is incorporated into HSPICE for the delay based analysis. The PUF signature is realized by exploiting the delay difference between the two paths. By having 128 such copies, we are able to obtain a 128-bit signature. It must be noted that the response in this example is static, and does not vary in w.r.t. the challenge-response methodology. Additionally, care must be taken to ensure correct termination to allow a reasonably accurate testing.

### *6.3.3 Qualitative and Quantitative Analysis*

In order to perform inter- and intra-PCB HD, it is necessary to first determine the min and max frequency between which the authentication signal frequency will be swept. This is based on the calculated resonance frequency. The frequency range between max and min is digitized with 2 N where N is the number of bits in response. The resonance frequency of each PUF is associated with its digital equivalent, i.e., min frequency is all 0 s and max frequency is all 1 s. This digitization will require either an embedded hardware or an external digitizer. By comparing the response generated between the various PCBs, the inter-PCB hamming distance is observed. Next, the arbiter-coil-based delay PUF is subjected to an inter-die HD analysis, additionally, by subjecting the PCB to temperature and moisture variations, the intra-PCB HD can be obtained.

## 6.4 Conclusions

PCB is a potential target of broad range of new attack vectors such as cloning, Trojan insertion, Modchips, and reverse engineering. PCB authentication brings new challenges that were absent in conventional IC authentication. We have shown that clever localized modifications in PCB during design or fabrication can evade conventional structural and functional testing. They can lead to malicious and often catastrophic outcomes during field operation. We have also presented two possible countermeasures through judicious trust validation and low-cost design approaches. With growing complexity of multilayer PCBs including hidden vias and increasing reliance on third-party resources, more complex Trojan attacks would become feasible. Due to the widespread use of PCBs, their vulnerability to Trojan attacks poses major concerns in trust and security of electronic products. Untrusted PCBs can enable highly sophisticated and powerful attacks such as unauthorized access to a system or wirelessly transmitting secret data. Aside from Trojan insertion, piracy via counterfeiting of PCBs pose a significant threat as well. In this chapter we presented a systematic methodology to authenticate the PCBs using PCB PUF.

**Acknowledgments** This work supported by Semiconductor Research Corporation (#2727.001), National Science Foundation (CNS-1441757), and Defense Advanced Research Projects Agency under award #D15AP00089.

## References

1. R.S. Chakraborty, S. Narasimhan, S. Bhunia, Hardware Trojan: Threats and Emerging Solutions. in *Proceedings of the IEEE International HLDVT Workshop*, pp. 166–171, 2009
2. PCB manufacturers look forward to Ultrabook and Wintel, http://www.chinapcbs.com/
3. Y. Alkabani, F. Koushanfar, Consistency-based characterization for IC Trojan detection, International Conference on Computer-Aided Design, 2009
4. H. Salmani, M. Tehranipoor, J. Plusquellic, A layout-aware approach for improving localized switching to detect hardware Trojans in Integrated Circuits, IEEE International Workshop on Information Forensics and Security (WIFS), 2010
5. F. Domke, Blackbox JTAG Reverse Engineering, http://events.ccc.de/congress/2009/Fahrplan/events/3670.en.html, 2009
6. K. Rosenfeld, R. Karri, Attacks and defenses for JTAG. IEEE Des Test Comput **27**(1), 36–47 (2010)
7. A. Hennessy, Y. Zheng, S. Bhunia, JTAG-based robust PCB authentication for protection against counterfeiting attacks. In Design Automation Conference (ASP-DAC), 2016 21st Asia and South Pacific (pp. 56–61). IEEE, January 2016
8. K. Rosenfeld, R. Karri, *Security and Testing, Introduction to Hardware Security and Trust* (Springer, 2012)
9. N. Asadizanjani, A new methodology to protect PCBs from non-destructive reverse engineering, in *42nd International Symposium for Testing and Failure Analysis* (6–10 November 2016). Asm
10. S. Ghosh, A. Basak, S. Bhunia, How secure are printed circuit boards against trojan attacks? IEEE Des Test **32**(2), 7–16 (2015)

11. S. Paley, T. Hoque, S. Bhunia, Active protection against PCB physical tampering, in *Quality Electronic Design (ISQED), 2016 17th International Symposium on,* pp. 356–361. IEEE, March 2016
12. Modchips: Wikipedia. [Online]. Available: https://en.wikipedia.org/wiki/Modchips
13. Printed Circuit Board Test Methodologies, http://download.intel.com/design/chipsets/applnots/29817901.pdf
14. J. Carlsson, *Crosstalk on Printed Circuit Boards*, 2nd edn., 1994
15. B. Sood, M. Pecht, Controlling Moisture in Printed Circuit Boards, IPC Apex EXPO Proceedings, 2010
16. G.E. Suh, S. Devadas, Physical unclonable functions for device authentication and secret key generation, in *Proceedings of the 44th annual Design Automation Conference* (ACM, 2007) pp. 9–14
17. L. Wei, C. Song, Y. Liu, J. Zhang, F. Yuan, X. Qiang, BoardPUF: Physical Unclonable Functions for printed circuit board authentication, in *Computer-Aided Design (ICCAD), 2015 IEEE/ACM International Conference on*, pp. 152–158. IEEE, 2015
18. F. Zhang, A. Hennessy, S. Bhunia, Robust counterfeit PCB detection exploiting intrinsic trace impedance variations, in *2015 IEEE 33rd VLSI Test Symposium (VTS)*, pp. 1–6. IEEE, 2015
19. A.S. Iyengar, Authentication of Printed Circuit Boards. In 42nd International Symposium for Testing and Failure Analysis (November 6–10, 2016). Asm
20. H. Rau, C.-H. Wu, Automatic optical inspection for detecting defects on printed circuit board inner layers. Int. J. Adv. Manuf. Technol. **25**(9–10), 940–946 (2005)
21. https://www.cadence.com/content/cadence-www/global/en_US/home/tools/allegro-downloads-start.html