CHAPTER

PCB AUTHENTICATION AND INTEGRITY VALIDATION

15

CONTENTS

15.1 PCB AUTHENTICATION

A counterfeit PCB typically differs in functionality, performance, or reliability, but is sold as an authentic one. Similar to ICs, PCBs typically rely on a long and globally distributed development cycle that connects multiple untrusted parties. As shown in Fig. 15.1, PCB life cycle may include design houses, manufacturers, board assemblers, testing partners, and system integrators. Due to increasing reliance on various third-party entities, PCBs are vulnerable to counterfeiting attacks. Counterfeiting

Hardware Security. https://doi.org/10.1016/B978-0-12-812477-2.00020-4

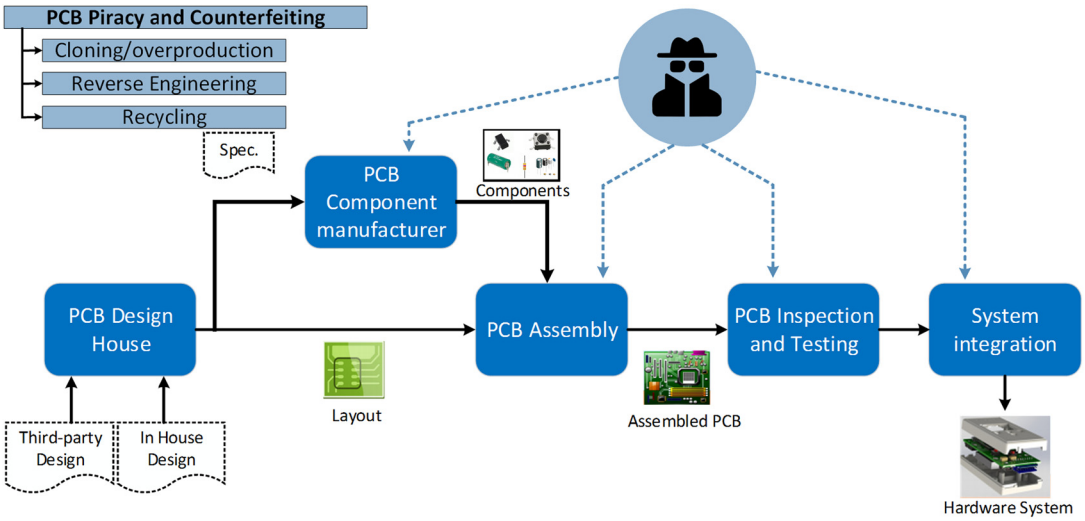

FIGURE 15.1

Typical stages in a PCB supply chain, which are vulnerable to counterfeit PCB insertion by an untrusted party through cloning, overproduction, reverse engineering, or recycling of discarded/used PCBs.

can be done by an untrusted third party, who obtains the layout of the PCB and generates a clone, or overproduces it. Furthermore, PCBs are relatively easier to reverse engineer compared to ICs, which again makes them highly vulnerable to cloning attacks by an adversary, who may not even have the PCB layout and specifications. Hence, counterfeiting of a PCB has become prevalent. Number of effective solutions have been reported to date to defend counterfeiting of ICs. However, existing chip-level integrity validation approaches cannot be readily applied to PCBs.

Counterfeit PCBs can be classified into various major categories. The most common form of counterfeiting is downright cloning of the complete PCB. This could be accomplished by an untrusted entity with access to the original design and specifications. As mentioned earlier, PCBs are mostly manufactured at untrusted fabrication facility. A bad actor in such a facility can clone or overproduce a PCB design. It could also be done by reverse engineering the bill-of-materials (BoM), and layout from a manufactured PCB deployed in the field. Further, discarded faulty PCBs from a PCB foundry or testing facility could be picked up by ghost shift workers in such factories. Those PCBs could be assembled with components, and then sold to customers as real products. Certain PCBs are bought, used, refurbished, and then sold as new, involving multiple parties in the process. The quality of these counterfeit PCBs may be poor, causing early failures, performance degradation, or potential damage, and loss of information to the end-users. This could happen because of the unreliable board material, or poor construction of such boards. The discarded and refurbished PCBs could be referred to as recycled PCB in the classification of counterfeit PCBs. These counterfeit PCBs can potentially have additional undesired functionalities, or malicious circuits, that is, Hardware Trojans [1].

Researchers have studied various PCB-specific parameters to create a unique and authentic board-specific signatures, which could be used for authentication of a PCB. The key idea is to obtain unique

identifying signatures after the PCB is manufactured. This is similar to the use of PUF in authentication of an IC through generation of unique fingerprint, as described in Chapter 12. This golden signature would be stored in a database. In the field, whenever the authenticity of a PCB needs to be verified, the signature of the PCB would be generated and compared with the golden reference. If the two signatures differ beyond a pre-determined threshold, the PCB would be marked as counterfeit, or unauthenticated. In this chapter, we present some of these signature-based authentication techniques. Section 15.2 presents different sources of variations that can be leveraged to extract the PCB signature. The methods of extracting signature are discussed in Section 15.3. Section 15.4 presents the metrics used for assessing the quality of the signatures. Finally, in Section 15.5, other potential authentication techniques are discussed.

15.2 SOURCES OF PCB SIGNATURE

Different physical, electrical, and chemical variations are introduced in a PCB by its manufacturing process. Such intrinsic sources of variations could be used for generating the authentication signature for a PCB. In the presence of a robust and unique signature, an authentic PCB could easily be differentiated from its cloned counterpart. Such an ideally, any signature to be used for authentication should have the following characteristics: 1) Random: the signature must be unpredictable; 2) Unclonable: signature of each unit would be unique and cannot be cloned by another; and 3) Robust: the signature should be captured reliably, even under varying environmental conditions (e.g., supply voltage, temperature). If the signature is extremely sensitive to environmental conditions, authentication may fail when such conditions vary. The above-mentioned desirable features would only be present in a signature if the source of variations inherently provide them. The entropy sources used in some of the intrinsic board-level signature generation techniques for PCB authentication are shown in Fig. 15.2 and discussed in the next section. Note that an alternative approach to PCB authentication is based on storing a device-specific unique identification number onto one-time programmable fuses inside a PCB. However, compared to the intrinsic counterpart mentioned above, extrinsic signatures are prone to various forms of invasive attacks, which may access and alter them. Such signatures are also vulnerable to cloning, where an adversary can deliberately assign them onto cloned PCBs.

15.2.1 TRACE IMPEDANCE VARIATION

PCBs typically consist of hundreds to thousands of metal traces distributed across the board (Fig. 15.3A). These metal traces are commonly made of copper (Cu) lines of different thicknesses. These traces are subject to random intrinsic manufacturing process variations, such as a random shift in length or width. Such differences cause variations in DC resistance, AC impedance, and signal propagation delay through these lines. Hence, the variation in trace impedance could be used for the board-level unique signature generation [2].

Two basic trace types of PCB are: (1) microstrip and (2) stripline. On a single layer PCB, the microstrip trace is the dominant type of trace for the underlying pattern of copper wire. However, in a multilayer PCB, both types of traces are used. Thus, different PCBs may have different wire impedance models, considering the copper trace and substrate dielectric. Cross-sections of these trace types are shown in Figs. 15.3B and 15.3C. Impedance (Z_0) of these traces rely on width and thickness

of the copper trace, thickness, and dielectric constant of the substrate. During the PCB manufacturing process, the dimensions of the traces would not be perfectly uniform in both width and height, and the dielectric constant of the substrate varies over the area of the PCB. These factors will result in a process-induced variation of the trace impedance. This impedance would vary from board to board and can be measured by a test equipment. Impedances from multiple traces in a board can collectively construct unique signatures from each board, which essentially acts as a PUF, and hence can be used for PCB integrity validation, or authentication.

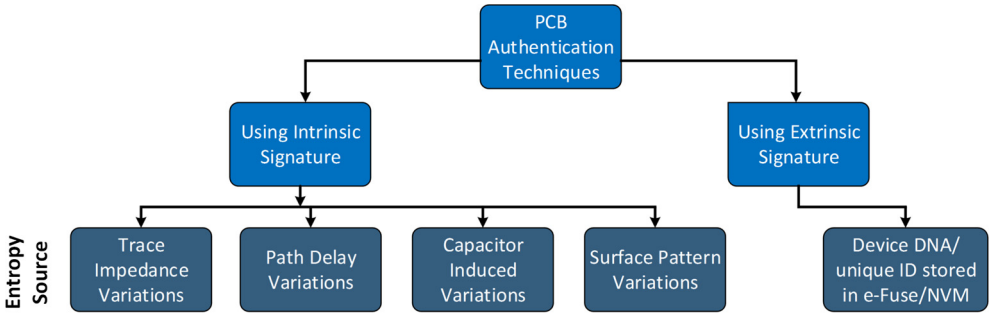

FIGURE 15.2

PCB authentication methods and corresponding entropy sources.

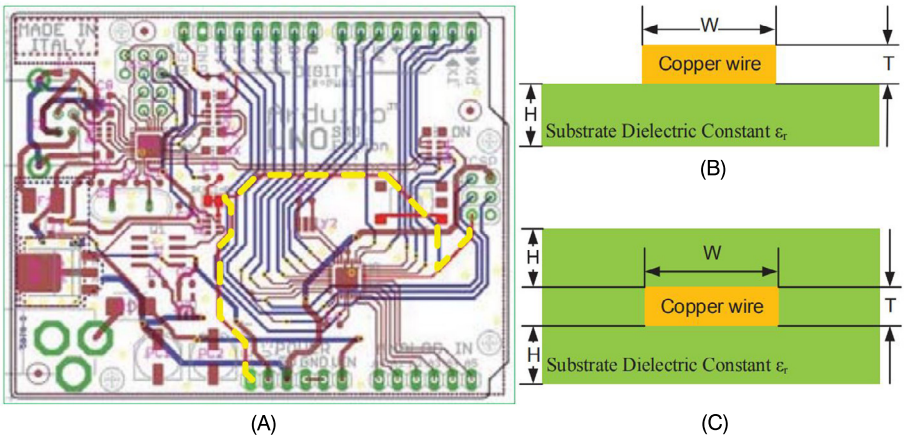

FIGURE 15.3

(A) The layout of the Arduino UNO R3 SMD Edition with a selected trace (highlighted in yellow [black in print version] dash line). Most PCB layouts contain a large number of traces similar to this; (B) Microstrip Trace in a single layer or multilayer PCB; and (C) Stripline Trace in a multilayer PCB.

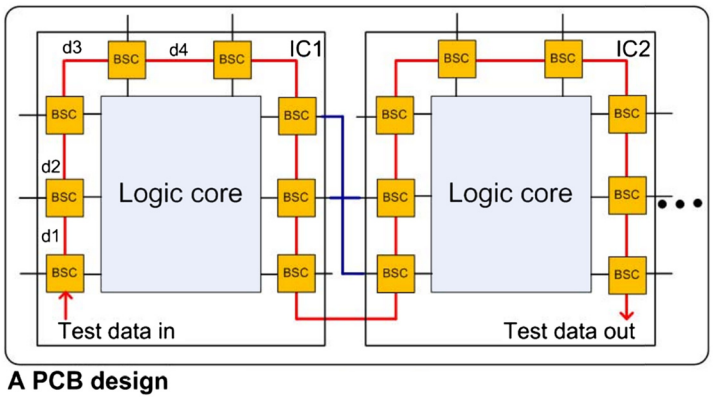

FIGURE 15.4

Boundary scan-paths surrounding the logic core of the ICs within a PCB design. The paths contain several scan cells connected in sequence.

15.2.2 DELAY VARIATION

PCBs can also be authenticated using high-quality delay-based signatures captured through the JTAG test infrastructure [3]. Boundary-scan chain architecture (BSA), inherent in most modern ICs, is a prevalent DFT structure used by the majority of PCBs today. As illustrated in Fig. 15.4, within this scan architecture several boundary-scan cells (BSCs) are connected in a chain. These BSCs are connected to one another in a manner identical to a shift register to form the boundary-scan register. They are used to shift specific test patterns to the logic core of an IC during the PCB testing process. The corresponding response of the IC under test can also be shifted out through the scan-chain. Multiple PCBs fabricated for a given design contain identical routing of the scan-path. However, data passing through identical scan-paths across different boards are still expected to experience a slightly different delay because of subtle variations in the manufacturing process of both the IC and the PCB. By measuring this delay of the BSC paths, a unique signature for authentication can be generated.

15.2.3 CAPACITOR-INDUCED VARIATION

One can include additional traces or components in a PCB, e.g., capacitive units, to deliberately introduce a source of entropy. They can be used to generate unique signatures in the manufactured boards. Such capacitive units could consist of a set of carefully-crafted copper patterns dedicated to maximizing manufacturing process induced variations [4]. Each capacitive unit could be incorporated with dedicated sensing hardware in the PCB. The sensing hardware outputs a signal that contains a specific frequency-value depending on the manufacturing variation of the corresponding capacitive unit. By comparing the frequencies extracted from these individual capacitive areas, a PUF logic can be implemented. To be able to ensure the generation of robust and distinguishable signature, each capacitive unit should contain a specific capacitance that experiences a large enough variation during manufacturing. At the same time, the capacitance should be large enough compared to on-board parasitics for providing noise immunity.

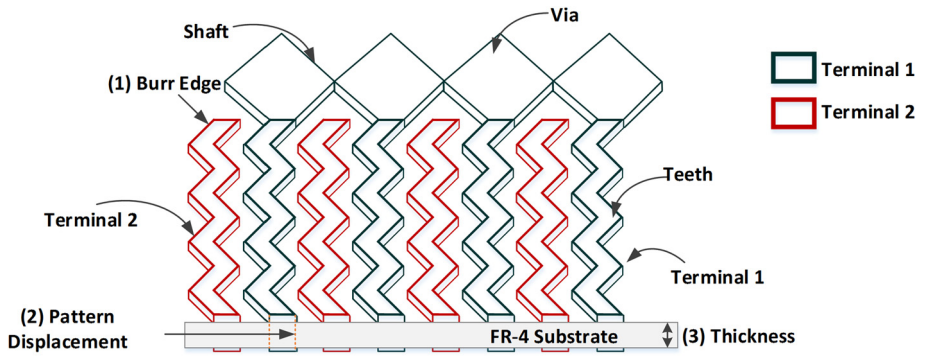

FIGURE 15.5

3-D representation of the two-layer comb-shaped trace pattern fabricated on PCB, acting as the capacitor that provides a source of variation for the signature generation process.

The capacitor unit could be designed in different layers of PCB, with a specific number of terminals, as shown in Fig. 15.5. These terminals may consist of copper traces drawn following a specific pattern that increases the chances of variation during manufacturing [4]. Researchers have tested zig-zag copper patterns (Fig. 15.5). Each layer would contain such patterns, and they could be connected with vias on the "shaft". This facilitates a "teeth-like" structure, where every "teeth" is surrounded by teeth of another terminal, creating sideward and vertical electrical field when charged. Furthermore, the capacitor units could be buried in the internal layers of PCB for noise immunity. Process-induced variations in different parameters introduce physical discrepancies in the trace patterns. These discrepancies could change internal electrical fields of capacitors and vary their capacitance values. Some of the manufacturing variations are the following:

- Misalignment of the pattern mask leading to varied shapes of copper patterns (local variation)
- Variation in chemical etching process (local variation)
- Different thickness of the boards (global variation)
- Subtle misalignment/shift within PCB layers (global variation)

Among the aforementioned variations, local variation refers to imperfections that impact individual units locally, whereas global variations indicate a boardwide impact.

15.2.4 SURFACE PATTERN VARIATION

Imperfections in the PCB manufacturing process could result in variations in visual surface patterns of the PCBs. This surface pattern variation can be used to generate the signature for PCB authentication. These visual patterns could be found in various observable components of the PCB, such as interlayer connecting vias, routing and power traces, surface mount devices (SMD), and pads [5]. Figure 15.6 illustrates some of these components in PCB. Interlayer connecting vias that are commonly found in all modern PCBs are basically small-plated holes in the PCB surface. These vias are used for several reasons, but their main purpose is to connect different PCB layers. Their quality has a crucial role in

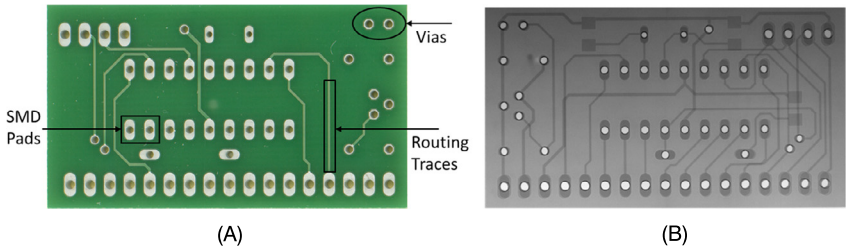

FIGURE 15.6

(A) Image of a PCB surface with vias, routing and power traces, SMD pads; (B) X-ray computer tomography image of the PCB surface [5].

assuring PCB quality. Surface pattern deviation of the vias could be contributed by several factors, including:

- Finishing process of the via surface
- Variation in drilled holes
- Separation between solder mask boundary, and via edges
- Angle present in the via hole (observable in 3D view)

The via surface of a PCB contains several small lines of different size, shape, and orientation. These variations could be observed in the microscopic image of a via. Figure 15.7 shows the patterns present in two vias [5]. Various randomly shaped/sized marks and dots can be observed on the surface, resulting from manufacturing process induced deviations. These random noise-like patterns could be leveraged

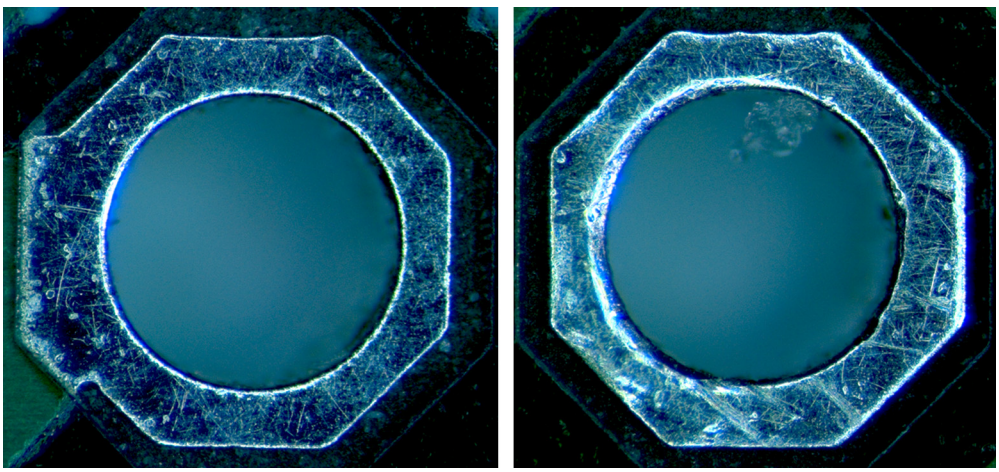

FIGURE 15.7

Randomly shaped/sized marks and dots on the via surface resulting from the manufacturing process [5].

to create a unique identifier for the PCB. Since via alignment is a very challenging task, it is unlikely to have no misalignments in all vias of a PCB during manufacturing. Hence, an abundant source of variation should always be present. Furthermore, the differences among visual surface patterns are absolutely unpredictable and cannot be controlled as well. Via-based surface fingerprints should be robust even under harsh environmental derivations. These via patterns also remain unused in the field and no electronic components are soldered over them. Finally, they provide excellent physical access for capturing surface patterns. Overall, surface vias have the potential to deliver unique and robust signatures for PCB authentication.

15.3 SIGNATURE PROCUREMENT AND AUTHENTICATION METHODS

While IC-level process variations have been extensively leveraged to implement PUFs [6], there has been a dearth of study exploiting board-level variations using such functions. In the absence of an effective signature extraction method, the underlying variation would not be utilized properly. The extracted signature for each PCB could be stored onto a central database during manufacturing, as shown in Fig. 15.8. A third-party facility other than the original manufacturer could also be hired for this enrollment process. In the field, to verify the authenticity of a given PCB, the associated signature extraction method has to be followed. The extracted signature needs to be sent to the central database to verify if that particular PCB is authentic. If the signature is present in the database, the PCB is verified to be authentic. Otherwise the PCB is deemed fake. Below, we discuss the corresponding signature generation and authentication methods developed for each source of variation discussed earlier in Section 15.2.

15.3.1 LEVERAGING PCB IMPEDANCE VARIATION

Automated test fixtures are commonly used in modern PCB production processes. Flying probes are used as the test fixtures that securely connect with test points in a design to provide quality assurances to the manufacturer and the system designer. For capturing the trace-impedance-based signature of a

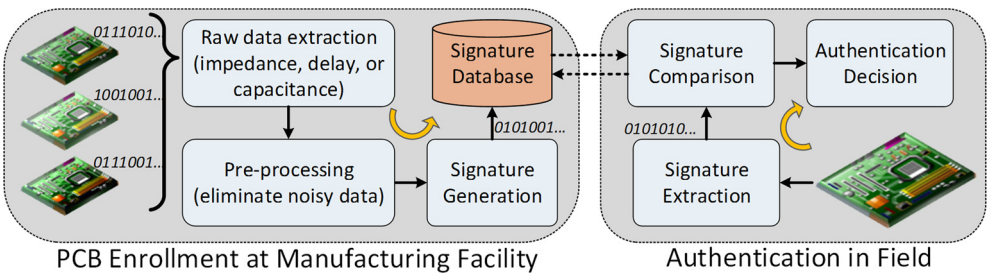

FIGURE 15.8

A generic flow of PCB enrollment and authentication process: during manufacturing, signature from each PCB is captured and stored in a central database. In field, the authenticity of a PCB can be verified by generating its signature and querying the central database.

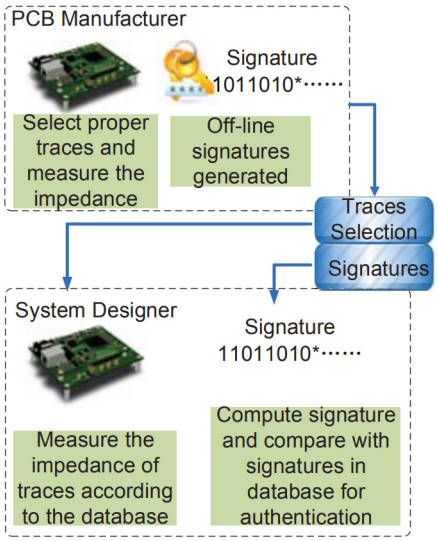

FIGURE 15.9

Overall steps of the trace-impedance-based PCB authentication procedure.

PCB, some of the existing probes could be used, or extra probes could be introduced to automatically measure impedance, and resistance of a set of predefined traces.

The overall approach of the trace-impedance-signature-based authentication method proposed in [2] is divided into two phases as shown in Fig. 15.9. In the first phase, an appropriate set of wire traces are selected by the PCB manufacturers. The impedance of those traces is measured under a stable frequency on all authentic PCBs. Signatures are produced off-line, based on the impedance measurements. The selection of traces and the corresponding signatures are stored in a database. In the second stage, system designers or end-users, who acquire the PCBs from the market need to measure the same selected traces for each PCB, and compute the signature, which is then compared to the signatures stored in the database. A PCB is determined to be counterfeit if the produced signature does not match with the one in the database.

Since PCBs contain hundreds of traces, a practical way to select traces for the signature generation would be to pick the ones that go through multiple vias. Recall from Chapter 4, that a via is a small hole drilled in a circuit board that connects the top layer of copper to the bottom layer. Each board manufacturer has a different process for etching the copper off the substrate, and drilling and plating the vias. These different methods have different intrinsic resistances associated with them. Hence, if the traces for signature generation are selected in an above-mentioned manner, the achievable randomness in signature could be maximized.

15.3.2 AUTHENTICATION USING DELAY VARIATION

Delay-based PCB authentication using JTAG is separated into two stages [3]. The flow is described in Fig. 15.10. In the first stage, a PCB manufacturer configures the JTAG device(s) on a PCB into an

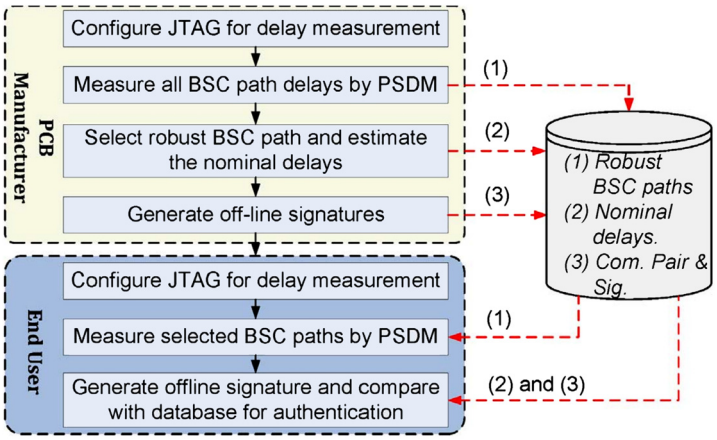

FIGURE 15.10

Major steps in the proposed JTAG-based PCB authentication process.

appropriate state needed to measure the delay of the BSC paths on all authentic PCBs. Some paths have fluctuating delay values when temperature or supply voltage vary. Those paths should not be selected in the signature generation process. Afterward, the signatures are produced off-line. The PCB manufacturer and end-user calculate the signature, based on the nominal delay value. A single bit of signature can be obtained by comparing the delay of two paths. For instance, when comparing path x and y with delay d_x and d_y, we can get a signature bit s as the follows:

$$s = \begin{cases} 1, & d_x > d_y, \\ 0 & \text{else.} \end{cases}$$

Following this technique, a large string of bits (that is, 256 bits) could be obtained as a complete signature for identifying every PCB. The locations of the BSC paths, the nominal delays, and signatures need to be stored in a central database. In the second stage, an end-user in the field needs to configure the JTAG on a PCB in the same way, and measure the delays of the selected BSC paths. Then, the signature is computed, which is compared with the signatures stored in the database. As before, the PCB is deemed to be counterfeit if the produced signature is not found in the database.

15.3.3 EXPLOITING CAPACITOR-INDUCED VARIATION

In order to generate an identifying signature from variations inherent to board capacitance, several capacitor units could be installed, as shown in Fig. 15.11. The capacitor units connect to measurement circuits through some auxiliary components. Each measurement circuit generates a signal that reflects the variation present in the corresponding capacitor unit through its frequency. The frequencies are typically different among capacitor units due to manufacturing process-induced deviations. Measured frequencies are compared in pairs to generate signature bits. A complete signature would have several bits, each generated from a unique frequency pair. These signature bits are permuted, based on a

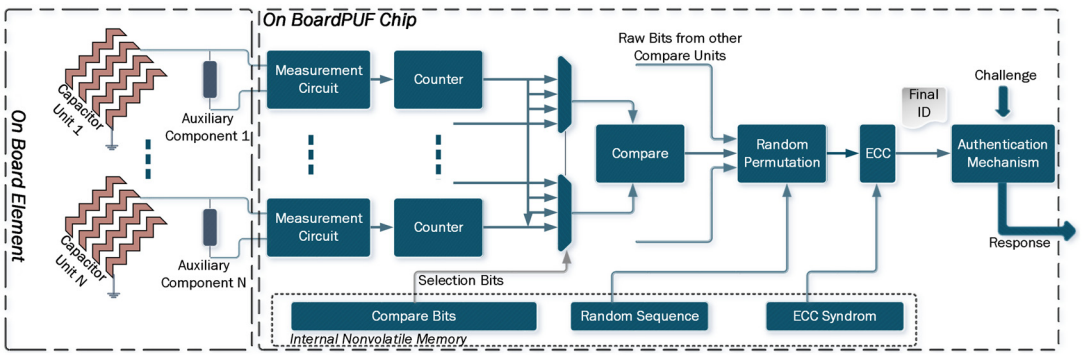

FIGURE 15.11

Extraction process of capacitance-induced variations and corresponding authentication technique using generated signatures.

pre-stored random sequence. The permuted signature represents the initial form of the PCB identity. It is worth noting that fluctuations in environmental and operational conditions may introduce errors in the generated identity, or signature. This initial signature is, therefore, corrected with the support of pre-stored error correction code (ECC), and the final signature is generated.

After manufacturing of the boards, an enrollment process is performed, where signatures for different challenge inputs are collected for each PCB. The challenge basically defines, which capacitor unit frequencies would be compared. Hence, for each PCB, several different challenge-response pairs are present, which is good in terms of security. During the enrollment process, different signatures for different challenges, with their corresponding random sequences could be stored in a database. During authentication in the field, the end-user verifying the board applies a specific challenge, and a signature for that given challenge is generated within the PCB. The correctness of the generated response is cross-checked with the one that was stored in the database during enrollment. If the signature is matched, the PCB would be considered authentic.

15.3.4 USING SURFACE PATTERN VARIATION OF PCB

To generate fingerprints from PCB surface patterns, high-resolution photos of the surface must be captured. Even minor surface details (for example, marks, texture, size, and shape distortion) must be captured in the pictures. Hence, the photos must be taken with high-resolution quality optics. The resolution is expected to be at least double the size of the target features [5].

It starts with the digitization of the PCB surface, using an appropriate imaging technique. The preprocessing step deals with noise present in the analog-to-digital conversion process [5]. The segmentation step deals with detection of signatures, providing regions within the PCB surface image. The next step computes the similarity between the suspect and the golden signature/fingerprint for a particular board. Finally, in the counterfeit detection step, a given test image is recognized as a counterfeit or authentic one. Since most electronic devices are covered with plastic covers, a technique to acquire the image during in-field authentication, without removing the cover, must be available. This could be

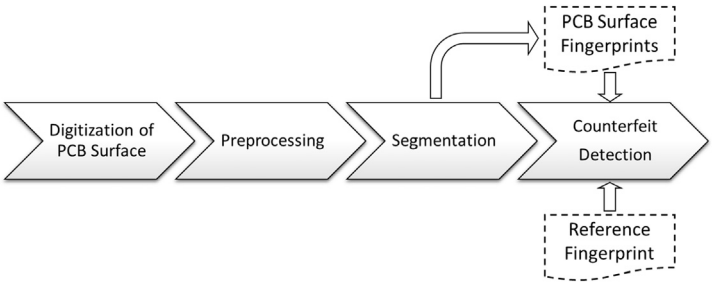

FIGURE 15.12

Various steps of the surface pattern variation based authentication process.

achieved by X-ray computer-tomography-based (CT-based) technique. Current industrial CT hardware can capture even minor details at micro-resolution. Figure 15.6B shows x-ray tomography image of a PCB surface. The subsequent steps for PCB surface authentication are shown in Fig. 15.12. Since the image-capturing process may encounter geometrical distortions, due to surface misalignment, a pre-processing step can be used. This step may involve averaging of several images, and further application of median filtering to reduce noise. It can greatly enhance the quality of the captured photos.

A template-matching scheme is applied to identify target regions within the captured image during the segmentation step. Since the region of interest for capturing the signature must be focused on a sub-region within the board, the segmentation step is crucial. Finally, the segmented region(s) can be used for signature generation in several ways. One way would be to extract quantitative values of several predetermined features from the target regions. If a large number of features are present, a signature could be obtained from that. However, existing methods directly use the isolated segment(s). During authentication, the segmented image of the target PCB is compared with golden one, using similarity measure techniques, such as normalized cross-correlation (NCC), which is commonly used for human fingerprints recognition.

The golden signature (segmented preprocessed surface image) for all authentic PCBs would be captured after the manufacturing process is complete. The captured signature would be stored in a database. During authentication in field, the NCC value of the golden and the target PCB image needs to be calculated. If the similarity is less than a pre-defined threshold, the PCB is considered to be different from the golden one. Hence, it would be detected as a counterfeit PCB.

15.4 SIGNATURE ASSESSMENT METRIC

The most common metric used for assessing the quality of signature-based-PCB-authentication schemes is the hamming distance (HD). HD is the amount of variation present within two signatures. To clearly distinguish between two boards, the HD of their signatures should be ideally 50%. This board-to-board signature variation is called inter-PCB HD. Likewise, the signature of the same board captured at two different time instances should ideally be the same. However, there are often some dif-

ferences, due to measurement and environmental variations. Hence, the within-the-board or intra-board distance of the signature should be very close to 0%.

Figure 15.13A shows the histogram of intra-PCB HD for several PCB signatures generated from trace impedance variations. It is evident that the distribution is primarily focused near 50% (0.5) HD area. Conversely, the intra-PCB HD is mostly 0%. Hence, the signatures generated from trace impedance appear to be unique and robust. A similar conclusion can be drawn for signatures generated from scan-chain path delays captured via JTAG (Fig. 15.14).

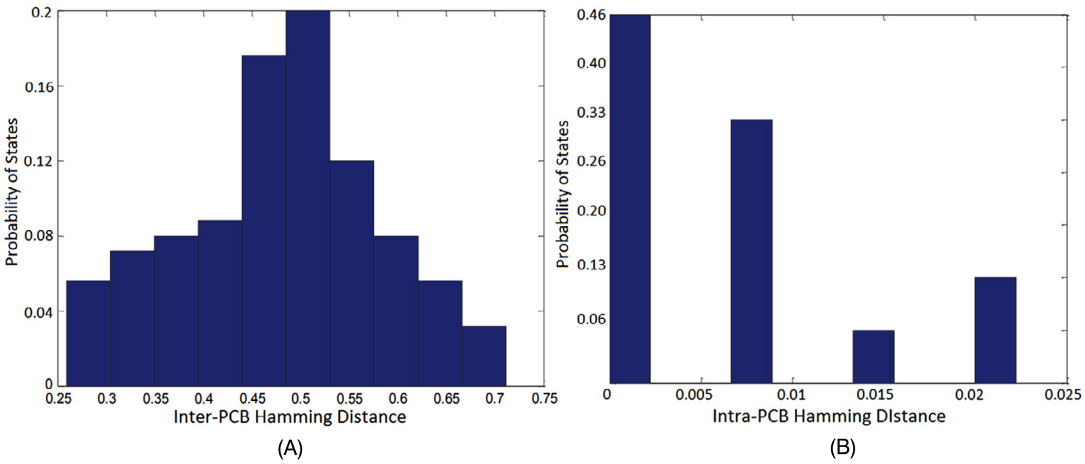

FIGURE 15.13

(A) Inter-PCB HD; and (B) Intra-PCB HD for signatures collected from trace impedance variations.

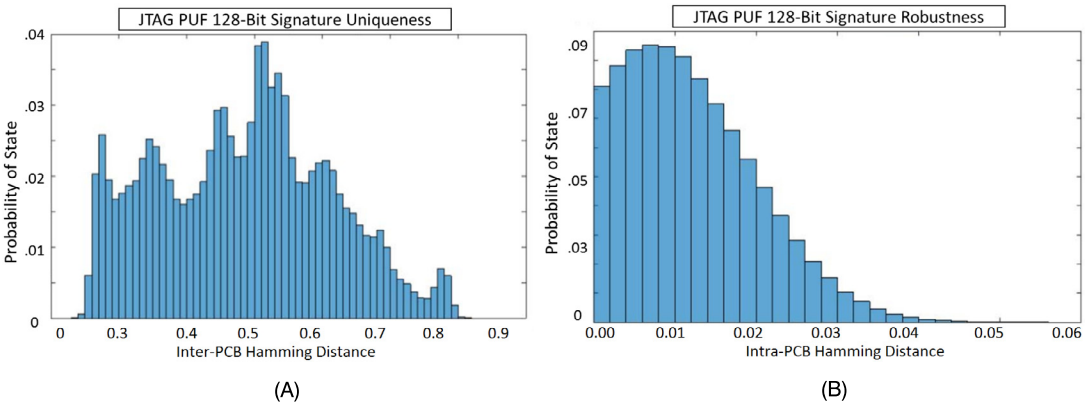

FIGURE 15.14

(A) Inter-PCB HD; and (B) Intra-PCB HD for signatures collected from delay variations.

15.5 EMERGING SOLUTIONS

15.5.1 SYSTEM-LEVEL MUTUAL AUTHENTICATION

A system-level mutual authentication approach can be used to authenticate both the hardware and firmware, as described in [8]. In this method, the hardware is used to authenticate the firmware by verifying the firmware's checksum during power-up. On the other hand, firmware can verify the identity of the hardware, and will not produce correct results, unless it receives a unique hardware fingerprint.

In this framework, a system ID (SID) is first generated after the PCB is assembled, and returned to the system designer. SID is created from the IDs of different chips (CIDs) present in a system, and is the XOR summation of these chip IDs. This ID is unique and resistant to cloning, as it is never exposed to the outside world. Once a system is assembled, each SID for a system is created and stored in a secure database at the trusted system integrator's site for future authentication. To prevent the use of cloned PCB, the firmware for the target hardware is obfuscated in such a way that it can only work upon receiving a correct system ID. Once the systems are manufactured and assembled, they must be shipped to the original system designer to compensate the obfuscated firmware.

When a system is powered-up in the field, it is necessary to construct the SID for proper operation. The in-system processing unit (e.g., processor, digital signal processor, FPGA, or microcontroller) is responsible for creating the SID. There is also a secure protocol for the processor to collect all the encrypted SIDs from the chips. The unique SID provides excellent protection for the hardware. If one of the ICs (including the processor) is replaced with a new one (recycled or low-grade counterpart having a different SID), it will be reflected in the SID. For the compromised system, the SID is never registered in the system integrator's database. The system ID provides an easy way of detecting a non-authentic hardware. However, it cannot prevent an adversary from creating this non-authentic hardware. On the other hand, an adversary cannot reconstruct an original firmware from the obfuscated one. Incorporating these two can prevent an adversary from creating a non-authentic system.

15.5.2 AUTHENTICATION USING RESONANCE FREQUENCY

A novel coil-like structure is proposed in [9] to capture different sources of variations to generate unique signatures for PCBs. Figure 15.15A shows the proposed coil structure. The assumption is that, due to the presence of a high number of notches, the proposed star-coil structure should provide increased resistance (wire resistance), capacitance (due to the comb-shaped multilayer design), and inductance (due to the coil shape) variation compared to typical straight-coil designs. Hence, this method can capture several sources of manufacturing imperfections, including edge rounding, density, and alignment variations.

The star-coil structure could be used for exploiting resonance frequency (RF), which is expected to be unique for each coil. The frequency of the star-coil can be swept from minima to maxima when a voltage is being applied to excite the coil. At a specific frequency, the current through the coil becomes maximum (that is, impedance becomes minimum). This frequency is considered as the resonance frequency. The following equation defines the resonance frequency for an RLC circuit:

$$f_{\text{res}} = \frac{1}{2\pi\sqrt{LC}}.$$

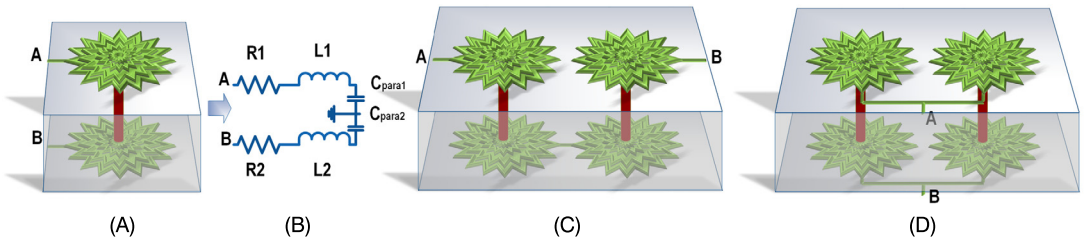

FIGURE 15.15

Star-coil structure: (A) base configuration, (B) equivalent RLC circuit, (C) series connected coils, and (D) parallel coil combination.

In the equation above, f_{res} refers to the resonance frequency in Hz, L is the inductance in Henry, and C refers to the capacitance in Farads. Since there is an inverse relationship between impedance and resonance frequency, a minute change in the impedance translates to a large change in the resonance frequency. Therefore, the value of f_{res} should be different across several boards. The single star-coil design can be extended by using multiple such coils connected together in a serial or parallel fashion (Fig. 15.15C–D). This would incorporate more variations, resulting in a large number of unique signatures.

The previous star-coil-based structure only provides one signature per board. Ideally, a secure and reliable authentication scheme would require a large number of challenge-to-signature pairs. To accommodate this feature, several stages of star-coils could be connected in various possible combinations to form a path through external jumpers. This connection combination could be defined with a challenge input during authentication, and the corresponding signature for each challenge (path configuration) would be unique.

15.6 PCB INTEGRITY VALIDATION

PCBs are an integral part of almost all electronic systems, including the ones that are responsible for performing various security-critical applications. Therefore, these boards are vulnerable to in-field alteration. The alteration can be caused by mounting ICs, soldering wires, rerouting paths to avoid or substitute existing blocks, adding or replacing components, exploiting traces, ports or test interfaces, and by many other ingenious ways. Circumventing digital rights management (DRM) by tampering with the PCB of a gaming console has been the most common example of PCB tampering [10]. Physical alteration to disable built-in restrictions allows the user to play pirated, burnt, or unauthorized versions of a game on the hacked console. One way to prevent such in-field alteration is to actively monitor the integrity of the PCB after deployment. However, there are very few methods available today for PCB integrity validation infield. Below we introduce some of these validation techniques.

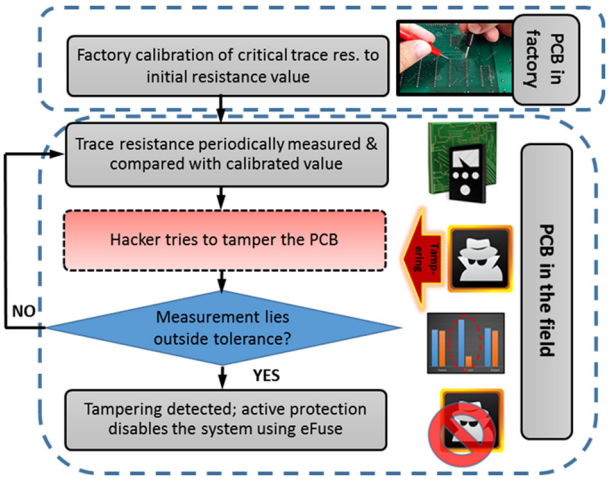

FIGURE 15.16

Block diagram showing the general approach of PCB security through sensing of trace resistance.

15.6.1 TRACE-IMPEDANCE-BASED VALIDATION

Copper traces within the PCB work as the interconnect among the components. In order to make any given component interact with the PCB, the component pins must be connected to some of the PCB traces in a direct or indirect manner. This could cause an observable change in the impedance of the copper trace. Hence, the impedance values of critical traces could be monitored to indicate this additional circuitry within the system.

In order to implement this method, the PCB vendor must collect the ideal trace impedance values for a large number of critical traces before deployment (Fig. 15.16). These impedance values must be stored within a nonvolatile memory, from which the values would be extracted and compared with the real-time measurements periodically—during operation—to ensure the integrity of the critical paths. Even the presence of a solder drop (used to connect wire/pins to the trace) would cause a measurable difference in the affected trace, and the tampering effort would be detected. The system could be equipped with features that disable the PCB as soon as a physical attack is identified.

15.6.2 JTAG-BASED INTEGRITY VALIDATION

JTAG-based PCB authentication method has already been discussed earlier in this chapter. The same idea could be extended for integrity validation purpose. Since the paths connecting the boundary-scan cells could be accessed through JTAG infrastructure, a board-specific signature could be extracted from the delays of these paths. Delay values from a large number of paths could be combined to create a unique signature of the board. Any modification that impacts any of these paths would lead to delay variations. Hence, if the ideal delay values of all scanpaths for a given board are known, that could be used to assess if any trace, pins, or component connected directly or indirectly to the JTAG chain has been tampered. The validation protocol could obtain the ideal values from a tamper-proof nonvolatile

memory, or from the cloud at system startup. Similar to the trace-impedance-based validation, the ideal delay values would be compared with the actual delay values of the board in a regular interval during operation. One important requirement of this technique is that the ideal delay values should be updated over a long period of operation, as the delay could change as the device ages.

15.7 HANDS-ON EXPERIMENT: PCB TAMPERING ATTACKS (MODCHIP)

15.7.1 OBJECTIVE

In this experiment, the students will have the opportunity to apply a physical attack, namely a Modchip attack, to a PCB to alter its functionality.

15.7.2 METHOD

Using the HaHa platform, the students will target modifying the behavior of the EEPROM, which stores the secret cryptokey. The first part of the experiment allows students to locate the main modules, observe the connectivity, and identify data/supply ports. Next, the students will incorporate a malicious design modification that forces the EEPROM to provide a forced cryptokey value to the target module.

15.7.3 LEARNING OUTCOME

By performing the specific steps of the experiments, the students will learn how to apply a Modchip attack, and learn how to minimally modify the system under attack to break its security primitives, and to cause the highest impact. They will also experience the challenges with respect to protecting a device against tampering attacks.

15.7.4 ADVANCED OPTIONS

Additional exploration on this topic can be done through the application of a more controllable tampering attack, for example, the ones which allow the attacker to control the key value sent to the modules, and more sophisticated change in the system behavior.

More details about the experiment are available in the supplementary document. Please visit: http://hwsecuritybook.org/.

15.8 EXERCISES

15.8.1 TRUE/FALSE QUESTIONS

1. A PCB cannot be reproduced for cloning purposes unless the attacker steals the original PCB layout from the manufacturer.
2. Most IC authentication techniques can be directly used for PCB authentication.
3. Identical traces within the same board would have identical path delay and impedance.
4. Boundary-scan chain architecture (BSA) can be used for enabling design-for-test (DFT) solutions.

5. Capacitor units implanted for signature generation could be buried into the internal layers of PCB for noise immunity.
6. Misalignment of the PCB layers during manufacturing only causes local variation of parameters (that is, trace impedance).
7. Vias are only used for connecting different layers of a PCB.
8. Though the sources of variation for various signature-based PCB authentication process is different, the signature extraction process is identical.
9. Change in signature due to environmental variations could be tackled by using error-correcting codes.
10. Presence of several unique signatures for a given PCB does not add any value in authentication.

15.8.2 SHORT-ANSWER TYPE QUESTIONS

1. Classify the different types of counterfeit PCBs.
2. What are some of the desirable features of a good signature for PCB authentication?
3. Why do multiple PCBs manufactured from the same design have variations in impedance and delay among identical traces?
4. What is the traditional use of boundary-scan chain architecture (BSA) in an IC or PCB design?
5. What are some of the manufacturing imprecisions that could cause the capacitance of the capacitor units implanted for PCB signature generation to be different?

15.8.3 LONG-ANSWER TYPE QUESTIONS

1. Describe two different possible sources of variation that could be used for PCB authentication.
2. Describe how variation in board capacitance could be leveraged for PCB signature generation and authentication.
3. Discuss the metrics that are commonly used for understanding the quality of signatures for PCB authentication.
4. How could a star-coil trace structure in PCB be used for designing physical unclonable functions? Can you come up with a similar novel structure to extract more variation from PCB? Describe your mechanism in detail.
5. When a PCB is deployed in a harsh environmental condition (for instance, extreme heat), the generated signature from the PCB could vary from its golden reference. What would be your mechanism to tolerate these errors?

REFERENCES

[1] S. Ghosh, A. Basak, S. Bhunia, How Secure are Printed Circuit Boards against Trojan Attacks? IEEE Design & Test 32 (2015) 7–16.
[2] F. Zhang, A. Hennessy, S. Bhunia, Robust Counterfeit PCB Detection Exploiting Intrinsic Trace Impedance Variations, in: VLSI Test Symposium (VTS), 2015 IEEE 33rd, IEEE, pp. 1–6.
[3] 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, IEEE, pp. 56–61.
[4] L. Wei, C. Song, Y. Liu, J. Zhang, F. Yuan, Q. Xu, BoardPUF: Physical Unclonable Functions for Printed Circuit Board Authentication, in: Computer-Aided Design (ICCAD), 2015 IEEE/ACM International Conference on, IEEE, pp. 152–158.

[5] T. Iqbal, K.-D. Wolf, PCB Surface Fingerprints based Counterfeit Detection of Electronic Devices, Electronic Imaging 2017 (2017) 144–149.
[6] G.E. Suh, S. Devadas, Physical Unclonable Functions for Fevice Authentication and Secret Key Generation, in: Proceedings of the 44th Annual Design Automation Conference, ACM, pp. 9–14.
[7] HuaLan Technology, PCB clone, http://www.hualantech.com/pcb-clone, 2017. (Accessed 3 December 2017), [Online].
[8] U. Guin, S. Bhunia, D. Forte, M.M. Tehranipoor, SMA: a System-Level Mutual Authentication for Protecting Electronic Hardware and Firmware, IEEE Transactions on Dependable and Secure Computing 14 (2017) 265–278.
[9] V.N. Iyengar Anirudh, S. Ghosh, Authentication of Printed Circuit Boards, in: 42nd International Symposium for Testing and Failure Analysis, ASM International.
[10] S. Paley, T. Hoque, S. Bhunia, Active Protection against PCB Physical Tampering, in: Quality Electronic Design (ISQED), 2016 17th International Symposium on, IEEE, pp. 356–361.