Robust Counterfeit PCB Detection Exploiting Intrinsic Trace Impedance Variations

Fengchao Zhang, Andrew Hennessy, and Swarup Bhunia
Department of Electrical Engineering and Computer Science
Case Western Reserve University, Cleveland, OH 44106, USA
Emails: {fxz67, ajb200, skb21}@case.edu

Abstract

The long and distributed supply chain of printed circuit boards (PCBs) makes them vulnerable to different forms of counterfeiting attacks. Existing chip-level integrity validation approaches cannot be readily extended to PCB. In this paper, we address this issue with a novel PCB authentication approach that creates robust, unique signatures from a PCB based on process-induced variations in its trace impedances. The approach comes at virtually zero design and hardware overhead and can be applied to legacy PCBs. Experiments with two sets of commercial PCBs as well as a set of custom designed PCBs show that the proposed approach can obtain unique authentication signature with inter-PCB hamming distance of 47.94% or higher.

Keywords: Printed Circuit Board (PCB), Piracy, Counterfeiting, Trust, PUF, Authentication

I. Introduction

A counterfeit electronic component is one that has a discrepancy in functionality, performance, and reliability - but is sold as an authentic one. Counterfeiting of Integrated Circuits (ICs) is a global issue and a growing multi-billion dollar industry [1]. There have been numerous studies on how to prevent, identify, or mitigate IC-level counterfeiting. Similar to integrated circuits, Printed Circuit Boards (PCBs), which are common to all electronic products, also share a long globally distributed supply chain involving multiple untrusted parties, as illustrated in Fig. 1 (a). Hence, PCBs are also vulnerable to different forms of counterfeiting attacks. The relative ease of PCB reverse engineering and piracy of a PCB design make it highly vulnerable to cloning attacks. Hence, counterfeiting of a PCB has emerged as a prevalent practice [2]. However, there has been a dearth of study on the prevention, identification, or mitigation of counterfeit PCBs.

Counterfeit PCBs can be categorized into three major classes. The first and the most obvious one is outright cloning of the entire PCB, often times with the identification of the Bill-of-Materials (BoM) included in the process, so that a functioning counterfeit product can be quickly brought to market. By acquiring a sample PCB, some manufacturer can duplicate it without the original design and layout through a reverse-engineering process [3]. The second class consists of legitimate PCBs that do not meet the standards of the target

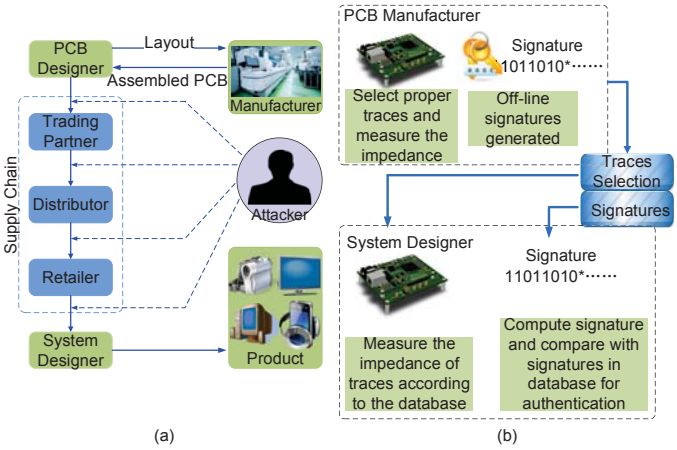

Fig. 1. (a) Typical stages in a PCB supply chain, which are vulnerable to counterfeit PCB insertion; and (b) overall steps of the proposed impedance based PCB authentication procedure.

customer and hence discarded. These PCBs can then by picked up by ghost shift workers in a factory; filled with components; and then sold to customers as real products. The final class of counterfeit PCBs is comprised of legitimate PCBs, which 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 due to the unreliable board material, poor layout, or construction. Furthermore, counterfeit PCBs can potentially have additional undesired functionalities or malicious circuits (i.e. Hardware Trojans) [11], which largely compromises the integrity of the resultant system.

Several counterfeit PCB detection approaches have been used in practice or explored in the research community. A method trademarked as "DNA marking" [4] was developed by Applied DNA Sciences, which embeds unique and unclonable botanical DNA on the products. This mark can be detected by laser readers down the supply chain. Such a technology, however, is simply able to detect the individual components (specifically chips) on the PCBs. This means that while the components soldered onto the PCB can be verified, the actual PCB itself cannot be. Radio Frequency Identification (RFID) and its variants constitute another technology platform, which

978-1-4799-7597-6/15/$31.00 ©2015 IEEE

is becoming popular in order to provide authentication to electronic products [5]. It relies on the wireless non-contact use of radio-frequency electromagnetic fields to transfer data for the purposes of identifying and tracking tags attached to objects. Though RFID is more robust over the traditional authentication mechanisms, it still suffers from the cloning problem – cloned RFID tags are indistinguishable from authentic ones. A final class of solutions for detecting counterfeit products is based on a security primitive called Physical Unclonable Function (PUF) [6] [7]. A PUF can extract a unique signature from each production unit of a design due to the random intrinsic manufacturing process variations. However, open literatures on the subject focus on a PUF embedded into a die or the IC package. They require special circuit structures (such as ring oscillators [6], memory array [7], or scan chain [8]) and hence, cannot be readily extended to PCB level.

We note that the metal traces on a PCB, typically numbering in the hundreds to thousands in a PCB of moderate complexity, can be powerful resources for PCB authentication. These metal traces,commonly made with copper (Cu) lines of different thickness, are subject to random intrinsic manufacturing process variations, such as random shift in length/width or contamination of Cu. Such variations reflect into variations of the DC resistance, AC impedance, and signal propagation delay through these lines. They vary from board to board and can be measured by a test equipment. Impedances from multiple traces in a board can collectively construct unique signature from each board, essentially acting as a PUF, and hence can be used for PCB integrity validation or authentication. A hallmark of modern PCB production processes is the set of automated test fixtures. Some of them use flying probes that securely make contact with test points in a design to provide quality assurances to the manufacturer and system designer. Some of the existing probes or extra probes added to the text fixtures can be used to automatically measure impedances and resistances of pre-defined traces for the purpose of PCB authentication. We observe that the DC resistance measurement is usually very sensitive to the exact contact condition between the probe and a PCB copper trace. However, measurement of the AC impedance of the copper traces is more robust. Moreover, since impedance $Z = \sqrt{R^2 + X_L^2}$, where $X_L = 2\pi fL$, L is the inductance and R is the resistance, it can capture variations in both resistance and inductance in the measured values.

In this paper, we propose a novel counterfeit PCB detection approach that utilizes the intrinsic impedance variations in metal traces on a PCB to create unique signature for authentication. It requires no design modification or hardware overhead. The overall approach is illustrated in Fig. 1 (b), which is separated into two stages. In the first stage, PCB manufacturers select apprpriate wire traces on the board and measure their impedances 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 bought 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 ones in the database. In particular, the paper makes the following key contributions:

1) It presents a novel methodology for PCB authentication, which does not require physical storage of key. Instead, it generates unique authentication signatures from each PCB exploiting random process variations that change the PCB trace impedances from board to board. Such an approach is low-cost requiring virtually no design changes or hardware overhead; and robust against invasive attacks (since no key is physically stored). To the best of our knowledge, this is the first key-less PCB integrity validation approach, and the first PCB PUF, which exploits intrinsic variations in PCB manufacturing process.
2) It evaluates the proposed authentication approach with two sets of widely used commercial PCBs. The experimental measurements show very high level of uniqueness and robustness of the signature for both sets of boards. In the experiment, 16 double-layer boards (Arduino UNO R3 SMD Edition) with the layout shown as Fig. 2 (a) [9] and 25 four-layer boards (Terasic DE0) were measured. We selected 10 traces on each board and each trace on the board was measured several times to minimize the impact of random measurement noise. For the Terasic DE0, 84 bits of unique signature were generated with the average inter-PCB Hamming Distance (HD) of 50.24% and intra-PCB HD of 2.14%. For the Arduino UNO, 120 bits of signature were generated with the average inter-PCB HD of 47.94% and intra-PCB HD of 1.06%.
3) To enhance the level of security as well as the ease of impedance measurements, it also presents a novel design-for-security (DfS) approach for PCB, which inserts carefully crafted trace patterns in a PCB design for the purpose of signature generation and authentication. We custom designed and fabricated such a PCB (30 copies) and measured all the trace impedances for all the copies. We observe very high level of impedance variations in these traces, which are suitable for signature generation with high entropy.

Remainder of the paper is organized as follows. Section II provides background on PCB wire impedance and motivation for the proposed solution. Section III describes the methodology of wire impedance based authentication. Section IV presents the measurement results and analysis. Section V presents a DfS approach for new PCBs. Section VI describes test apparatus that can be used in production to implement the proposed authentication. We conclude in Section VII.

II. Background and Motivation

PCB copper traces have resistive, inductive and capacitive effects distributed throughout them. Two basic trace types of PCB are the microstrip and stripline. On a single layer PCB,

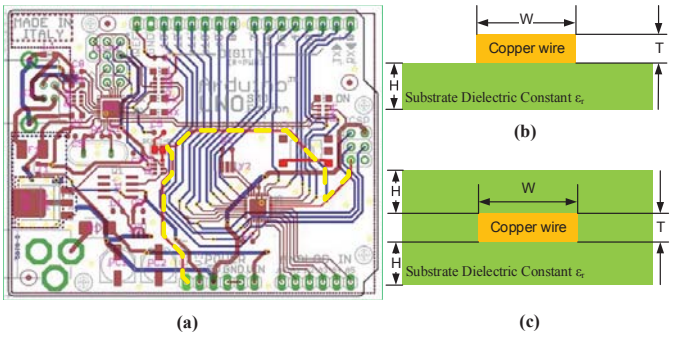

Fig. 2. (a) The layout of the Arduino UNO R3 SMD Edition with a selected trace (highlighted in yellow dash line); (b) microstrip Trace in single layer or multilayer PCB; and (c) stripline Trace in a multilayer PCB.

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 when considering the copper trace and substrate dielectric. Cross-sections of these trace types are shown in Fig. 2(b) and Fig. 2(c).

Impedance of a microstrip trace can be calculated as [10]:

$$Z_0 = \frac{87}{\sqrt{\epsilon_r + 1.41}} \ln\left(\frac{5.98H}{0.8W + T}\right) \quad (1)$$

Impedance of a stripline trace can be calculated as [10]:

$$Z_0 = \frac{60}{\sqrt{\epsilon_r}} \ln\left(\frac{4(2H + T)}{0.67\pi(0.8W + T)}\right) \quad (2)$$

Where Z_0 is the unit length characteristic impedance. From equations (1) and (2), the impedance of unit length is determined by width and thickness of the copper trace, thickness and dielectric constant of the substrate. During the PCB manufacturing processes, the dimensions of the traces cannot be exactly uniform in both width and height as well as the dielectric constant of the substrate varying over the area of the PCB. These factors will result in process-induced variations of the unit length impedance of a trace.

A flying probe test provides the feasibility to automatically and precisely measure the impedance of metal traces on a PCB. The test harness provides support for any number of probes to perform the analogue measurements of resistance, impedance, and inductance. In our experiments, a scaled down harness was built to fulfill the testing needs.

III. Methodology

In order to achieve a trace impedance based PCB authentication, or PCB PUF, first, we need to select a set of appropriate traces from a PCB design. Most PCBs are made using an FR4 substrate with so-called "One Ounce Thick Copper". This is defined as one ounce of copper spread over a square foot. Furthermore, some PCBs are bathed in molten tin or gold after fabrication (known in the industry as plating). This will result in difference in related parameters. For example, under room temperature, gold has a resistivity of 2.44×10^{-8} ohm·meter, while tin has a resistivity of 1.09×10^{-7} ohm·meter, almost an order of magnitude higher. If the original specifications for a PCB called for gold plating and a counterfeit PCB used cheaper tin plating, the counterfeit one will have a higher trace resistance. The difference cannot however be detected visually because during PCB assembly, solder covers up the gold plating and a PCB with gold plating will look indistinguishable from one with tin plating.

A measurable way to determine the authenticity of a PCB is through measuring the impedance of a trace that passes through multiple vias. A via is a small hole drilled in a circuit board that, when plated with metal, connects the top layer of copper to the bottom layer of copper. For PCB with more than two layers, there are two more types of vias. A blind via is a via that connects one of the outer layers of the PCB to one of the inner layers, while a buried via is a via that connects two of the inner layers together.

Each manufacturer of PCB starts with a similar piece of copper clad and they use their knowledge and skill to make the finished product. Each board house has a different process for etching the copper off of the substrate as well as drilling and plating the vias. These different methods have different intrinsic resistances associated with them. For example, a via that is electrochemically plated onto the FR4 will have a lower resistance than a via that is riveted on. Finding a good path for impedance measurement needs to consider many variables and factors. First, we need to ensure that two probes can make good contact with the path. Often times PCB designers coat their PCB in solder mask (a typically green substance that helps keep solder where it belongs) and silkscreen (a typically white paint that helps designate areas of the PCB). Both silkscreen and solder mask have a very high electrical resistivity, preventing an accurate measurement of the trace impedance. Furthermore, for multilayer PCBs such as Terasic DE0, many traces ran exclusively in the inner layers of the PCB, using blind and buried vias to travel through the PCB without ever touching the outer layers. These traces cannot be used for measurement, because they are hard to probe.

Once the traces are selected, the impedance can be measured by commercial instruments, such as an Keysight 4263B LCR Meter [13]. The LCR meter needs to be self-calibrated before measurement. Additionally open connection correction needs to be done (leaving the two probes disconnected from everything) along with short connection correction (shorting the two probes together). As shown in Fig. 3 (a), probes need to be carefully placed on the pad of a PCB to avoid unwanted contact with other pads on the PCB. Gold-plated probes should be used to obtain the lowest possible parasitic resistance and to maintain the contact between the probes and the pads.

A possible setup for trace measurement is shown in Fig. 3 (b). The impedance of each trace needs to be measured and data collected by averaging over a number of measurements (five in our case) in order to mitigate the effect of random measurement noise. In Step 1, we select total n paths and measure their impedances on PCB c to create a set $d^{(c)} = [d_1^{(c)}, d_2^{(c)}, ..., d_n^{(c)}]$. In Step 2, we compare

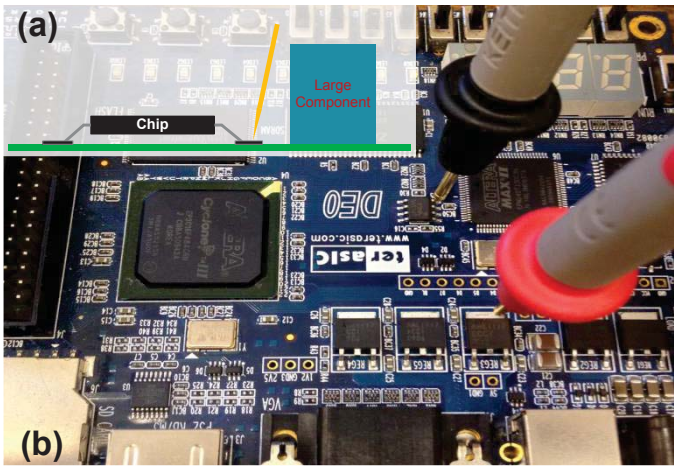

Fig. 3. (a) Schematic showing probe placement on a PCB substrate; (b) Terasic DE0 PCB measurement setup.

the impedances between any two paths on the same PCB by computing the distance between them. We then compute the vector $\overline{\Delta d^{(c)}}$ including $n(n-1)/2$ distance values (such as, $d_1^{(c)} - d_2^{(c)}$ and $d_1^{(c)} - d_3^{(c)}$). Thus, we get $\Delta d^{(c)} = [\Delta d_1^{(c)}, \Delta d_2^{(c)}, ..., \Delta d_{\frac{n(n-1)}{2}}^{(c)}]$. In Step 3, the normalization is done as: $\overline{d^{(c)}} = (\Delta d_i^{(c)} - min\Delta d^{(c)})/(max\Delta d^{(c)} - min\Delta d^{(c)})$. In Step 4, we select k specific bits (between i-th and j-th bit position) of the normalized values, to obtain $dig_{i,j}(\overline{\Delta d^{(c)}})$. We discard few least significant bits, which are highly vulnerable to environmental variations, as well as few most significant bits, which have poor variations. Finally, in Step 5, we combine the select bits from all normalized distances to generate a PCB signature of $k*n*(n-1)/2$ bits.

IV. Results and Analysis

We have evaluated the proposed approach with two widely used commercial PCBs - in particular, sixteen Arduino UNO R3 Edition double-layer boards and twenty five Terasic DE0 four-layer boards. For both set of boards, first we judiciously selected a set of total 10 traces. Next we performed impedance measurements at room temperature, $25°C$, for each trace for five times and averaged the values to eliminate random noise. Based on the measured impedances for each PCB, we generated the authentication signatures. Similar to other PUFs, the uniqueness and robustness were evaluated by the Hamming Distance (HD) metric. Assuming $HD_{i,j}$ stands for the Inter-PCB HD between PCB_i and PCB_j, the average inter HD for m PCBs, denoted by HD_{avg}, was calculated as:

$$InterHD_{avg} = \frac{2}{m(m-1)} \sum_{i=1}^{m-1} \sum_{j=i+1}^{m} HD_{i,j} \qquad (3)$$

In our experiment, we observed HD_{avg} of 50.24% based on 25 Terasic DE0 boards. Fig.4 (a) shows the histogram plot. The inter-PCB HD centers at around 50%, and ranges from 25% to 75%. As a result, the authentication of each PCB can be completed successfully with good uniqueness of their signatures.

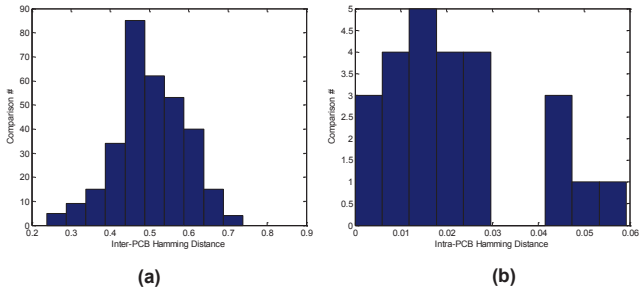

Fig. 4. (a) Inter-PCB HD; and (b) intra-PCB HD for Terasic DE0.

The robustness of the signature was evaluated under room temperature at two different times, which means the environment conditions, such as temperature, humidity and noise floor as well as the accuracy of the measurement setup were likely to vary between the two measurements. Assuming $HD_{p,q}$ stands for the intra HD of all boards between the pth measurement and qth measurement, the average intra-PCB HD for n times measurements on m PCBs, denoted by $IntraHD_{avg}$ was calculated as:

$$IntraHD_{avg} = \frac{2}{mn(n-1)} \sum_{1}^{m} \sum_{p=1}^{n-1} \sum_{q=p+1}^{n} HD_{p,q} \qquad (4)$$

The distribution of intra-PCB HD is shown in Fig. 4 (b) with an average of 2.14%. The Arduino UNO R3 boards were evaluated in the same way. The histogram of inter-PCB HD is shown in Fig. 5 (a) with an average of 47.94% in the range between 25% to 70% and the histogram of intra-PCB HD is shown in Fig. 5 (b) with an average of 1.06%.

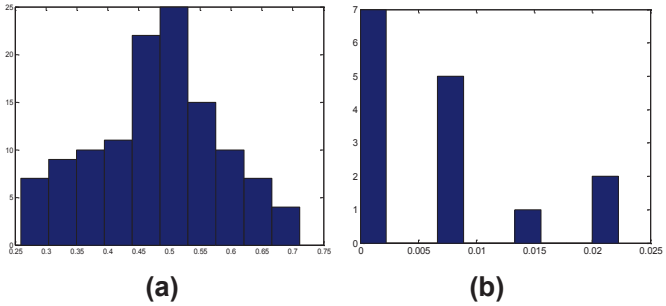

Fig. 5. (a) Inter-PCB HD; and (b) intra-PCB HD of Arduino UNO R3 SMD.

The average value of intra-PCB and inter-PCB Hamming Distance for both Arduino UNO R3 SMD and Terasic DE0 are shown in Table. I.

TABLE I
Measured results on inter and intra-PCB Hamming Distance

PCB Type	Avg. Intra-PCB HD	Avg. Inter-PCB HD
Terasic DE0	2.14%	50.24%
Arduino UNO R3 SMD	1.06%	47.94%

The signature is generated from the copper traces on the PCB with statistical variations inherent in the manufacturing processes. Considering the large number of traces which can be used for authentication, it's practically infeasible to fully clone the signatures in cloned PCB instances. Even if the distributions are copied, if the number of traces for authentication is large enough, the signature is still practically unclonable. Therefore, the trace impedance based authentication is an effective and secure method. The end user can identify a cloned PCB by producing its signature and compare it with the manufacturer's database.

V. Design for Security

The methods described thus far in this paper have been geared towards identifying counterfeit, particularly cloned PCBs, already in production. However, it is possible to design a new PCB with a set of additional traces (and access points to facilitate probing) built in to help identify cloned boards. The impedance values for these additional traces can be easier to measure. They provide new and potentially better source of entropy as well. Since these traces are not used for signal propagation, they can be designed to suffer from increased variations. Furthermore, since they are not used for PCB operation, they are less likely to suffer from wearing or aging effects. Hence, signatures generated from these additional traces can be more robust against aging effects.

It is very likely that a cloned PCB will be made using a cheaper method than the original. If the copper in the original circuit board was milled away while the cloned circuit boards copper was etched out, then a properly designed board would have traces that were well designed for a mill while being poorly designed for an etching process. For example, both processes of fabricating a PCB will have issues in making a large obtuse angle. A milling process will have issues making the inner section of the angle while an etching process will have issues making the outer portion of the angle. This will affect the measurement properties of the trace when viewed as a micro strip.

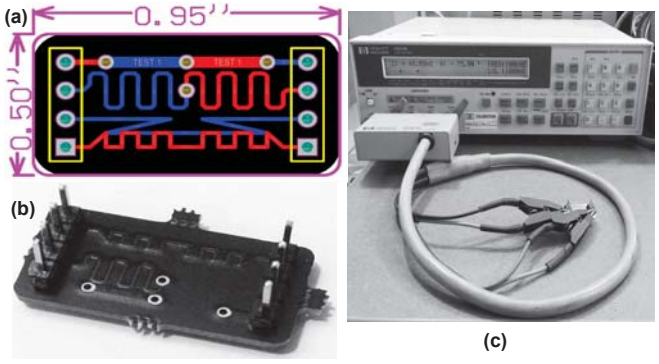

Fig. 6. (a) Suggested PCB authentication trace patterns in 0.5 square inches of PCB substrate; (b) photograph of the fabricated PCB with authentication patterns; and (c) measurement setup for these additional patterns.

Fig. 6 (a) shows a sample pattern that can be deployed to PCBs taking up less than 0.5 square inches. This pattern consists of four independent traces. Each trace was designed to take advantage of limitations in cheaper PCB manufacturing processes. The top trace, Trace 1, uses four differently sized micro strip transmission lines, each one transitioning between sizes (and layers) with the use of a via. The second trace, Trace 2, simulates a controlled impedance transmission line. The third trace, Trace 3, utilizes sharp angles to expose the afore-mentioned weaknesses in the manufacturing process. The final trace, Trace 4, continues to expose weaknesses in the manufacturing process by having numerous sharp right angle bends in the trace path. If tested at a high frequency, then variances in the process can be effectively exposed. Finally, the Trace 3 and Trace 4 partially overlap on different layers of the PCB, enabling the characterization of crosstalk.

Using the design in Fig. 6 (a) 30 PCBs were manufactured by OSHPark to test the uniqueness and robustness of the signatures generated by the judiciously designed traces. A photograph of one of the fabricated PCBs is provided in Fig. 6 (b).

Each of the four traces were tested using the same methodology described in Section III. The testing setup is shown in Fig. 6 (c). The average trace impedance for Traces 1 – 4 are 9.93 mΩ, 39.76 mΩ, 15.26 mΩ, and 22.38 mΩ with a standard deviation of 0.82 mΩ, 2.44 mΩ, 1.13 mΩ, and 2.44 mΩ, respectively. It can be observed in Fig. 7 (a) to (d), which show the trace impedance histograms for the four traces.

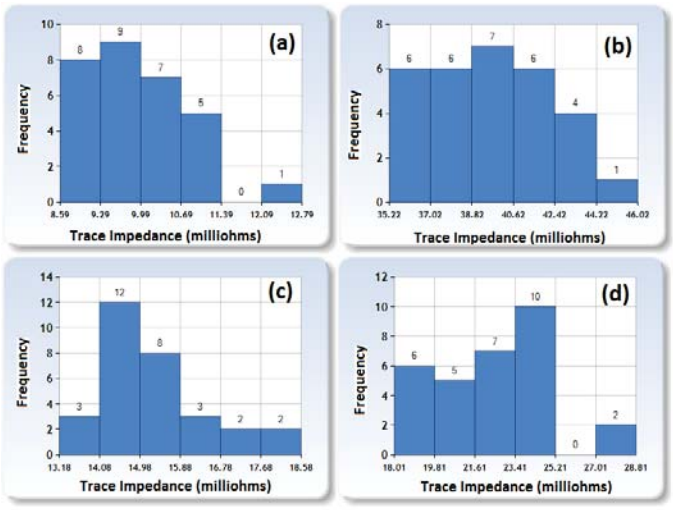

Fig. 7. OSHPark trace impedance histogram for: (a) Trace 1; (b) Trace 2; (c) Trace 3; and (d) Trace 4.

We observed that each of the four traces in the custom designed test PCB had a distinct signature that was easily measured by the test equipment. This is especially evident with the difference between Traces 2 and 3 (as shown in Fig. 7 (b) and Fig. 7 (c)) which have a similar histogram profile, however, Trace 2's resistance is almost three times greater than Trace 3's measured values. From these designs, it can be inferred that an individual trace can be identified from a group of traces and these traces provide high signature entropy.

VI. Impedance Measurement

In modern automated PCB production systems, one of the most important aspects is testing. This can range from test engineers physically handling the product to visually inspect for defects to robots probing the inner workings of the product for imperfections. In this section, we describe a system to fully implement the method of PCB identification and authentication described in Section III using automatic test equipment.

A common and effective PCB testing method is known as "flying probe" method of testing. Because the probes are on what is essentially an X-Y table, they can be moved into any position at any angle, allowing the probing of components such as ones depicted in Fig. 3 (a). Additionally, the probe heads are replaceable and four-wire probe heads, commonly called Kelvin Probes, are able to be attached to the "flying probe" system [12].

If we replace the heads of any common "flying probe" system with the heads described in [12] and attach them to any production-grade Micro-Ohm Meter, such as the Keysight 34420A, then very accurate and precise measurements of trace impedance can be taken. Next, through the use of the IEEE 488 General Purpose Interface Bus to communicate with a computer, the signature of a PCB under test can be automatically generated and verified without any user input [13].

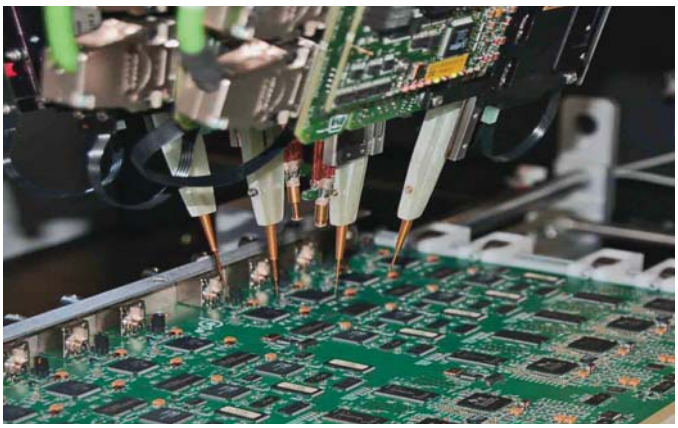

Fig. 8. An example of a commercial flying-Probe based In-Circuit Tester (ICT) [15].

One example of the aforementioned solution that is used in production today is the Keysight Technologies, Inc. *Medalist* i3070 Series 5 In-Circuit Test System [14]. This is an integrated all-in-one flying probe-based tester, an example of which is shown in Fig. 8. One of its key features is a unique system where an user can add-in custom measurement cards and software solutions. The i3070 supports finding points on the Device-Under-Test (DUT) either manually or by programmed knowledge of the Device-Under-Test [14]. By combining these two features, accurate impedance measurements can be preformed automatically. Using these measurements a signature for a specific PCB can be created. Finally, by communicating with a central server the signature can be saved for future verification by an end-user.

VII. Conclusion

We have presented a low-cost and robust approach to check PCB integrity in presence of counterfeiting attacks, in particular, cloning attacks. It relies on intrinsic manufacturing variations in metal traces of a PCB to create unique authentication signature from each PCB instance. Through detailed experimental analysis with common commercial boards, we have shown that the approach can be highly effective in robust PCB authentication. A major advantage of the proposed approach is that it does not require design modification or hardware overhead. We have shown that impedance measurements from 10 or more traces can provide adequate entropy for authentication. Existing production PCB testing setup can be used to automatically measure trace impedances for this purpose. We have also presented a DfS solution, where a PCB designer inserts carefully crafted additional wire traces, which are easier to measure and hidden from a board's surface. They simplify the authentication process and enhance the entropy.

VIII. Acknowledgement

This work is funded in part by National Science Foundation grants #1245756 and #1054744.

References

[1] "Defense Industrial base Assessment: Counterfeit Electronics", Bureau of Industry and Security, U.S. Department of Commence, Jan. 2010.

[2] "Integrated circuits china Manufacturer", BLD Electronic Co., Ltd. Available: http://dlbld.en.alibaba.com/product/954988019-215979726/integrated_circuits_china_Manufacturer.html

[3] "PCB Clone, PCB Copy, PCB Cloning, PCB Copying, PCB duplicating — PCB Reverse", HuaLan Technology. Available: http://www.hualantech.com/pcb-clone

[4] "DNA Marking and Authentication: A unique, secure anti-counterfeiting program for the electronics industry", *Applied DNA Sciences*, Stony Brook, NY, USA.

[5] S. Devadas, *et al*."Design and implementation of PUF-based "unclonable" RFID ICs for anti-counterfeiting and security applications", *EEE International Conference on RFID*, 2008.

[6] G.E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation", *DAC*, 2007.

[7] A.R. Krishna, S. Narasimhan, X. Wang, and S. Bhunia, "MECCA: A Robust Low-Overhead PUF Using Embedded Memory Array", *CHES*, 2011.

[8] Y. Zheng, A.R. Krishna, and S. Bhunia, "ScanPUF: Robust ultralow-overhead PUF using scan chain", *ASPDAC*, 2013.

[9] "ArduinoBoardUno". Available: http://arduino.cc/en/Main/ArduinoBoardUno

[10] "Design Guide for Electronic Packaging Utilizing High-Speed Techniques", 4th Working Draft, IPC-2251, February 2001.

[11] S. Ghosh, et al., "How Secure Are Printed Circuit Boards Against Trojan Attacks?", *IEEE Design & Test of Computers*, 2014.

[12] J.E. Boyette et al., "Dual-contact probe tip for flying probe tester", *US Patent 6023171*, February 8, 2000.

[13] Keysight 34420A NanoVolt/Micro-Ohm Meter, Available: http://literature.cdn.keysight.com/litweb/pdf/5968-0161EN.pdf

[14] Keysight *Medalist* i3070 In-Circuit Test System, Available: http://www.keysight.com/en/pc-1041067

[15] "ICT without Expensive Fixtures ACDI Expands Capabilities with In-House Flying Probe Tester", American Computer Development, Inc., 2011.