Accepted for publication: IEEE 51st International Carnahan Conference on Security Technology, Oct 2017
SAND2017-7175C

Unique Signatures from Printed Circuit Board Design Patterns and Surface Mount Passives

Jason R. Hamlet, *Senior Member*, Mitchell T. Martin, *Member*
Sandia National Laboratories
Albuquerque, NM USA
{jrhamle, mmart26}@sandia.gov

Nathan J. Edwards, *Member*
The MITRE Corporation
McLean, VA USA
nedwards@mitre.org

***Abstract*—Counterfeiting or surreptitious modification of electronic systems is of increasing concern, particularly for critical infrastructure and national security systems. Such systems include avionics, medical devices, military systems, and utility infrastructure. We present experimental results from an approach to uniquely identify printed circuit boards (PCBs) on the basis of device unique variations in surface mount passive components and wire trace patterns. We also present an innovative approach for combining measurements of each of these quantities to create unique, random identifiers for each PCB and report the observed entropy, reliability, and uniqueness of the signatures. These unique signatures can be used directly for verifying the integrity and authenticity of the PCBs, or can serve as the basis for generating cryptographic keys for more secure authentication of the devices during system acquisition or field deployment. Our results indicate that the proposed approaches for measuring and combining these quantities are capable of generating high-entropy, unique signatures for PCBs. The techniques explored do not require system designers to utilize specialized manufacturing processes and implementation is low-cost.**

Keywords—Authentication, integrity, hardware security, physical unclonable function, cryptographic key generation, anti-counterfeit

I. Introduction

The globalized supply chain has increased the complexity and difficulty of protecting critical systems such as avionics, medical devices, military systems, and utility infrastructure while ensuring their overall reliability. Subsequently counterfeiting or surreptitious modification of electronic systems during development or field operation is of increasing concern, especially for critical infrastructure and national security systems. In particular, detecting circuit-board level intrusions, and guaranteeing system integrity and authenticity have yet to be fully addressed in deployed systems. Much existing work to address these issues utilize Physical Unclonable Functions (PUF), tamper prevention technologies, or cryptographic algorithms in hardware or software built into the critical component silicon technology as in [1]. PUFs are physical characteristics of a device that are relatively easy to measure but difficult to reproduce. Often, they arise from variations in the manufacturing process that result in unique characteristics of individual devices. Amongst other uses, signatures derived from PUFs have found application in key generation and authentication, protecting intellectual property, and in enhancing the security of physical seals [2]-[5]. Previous efforts have focused on using PUFs to generate signatures for individual microelectronic devices, such as integrated circuits (ICs) and field programmable gate arrays (FPGAs). However, if the circuit board or other non-secure peripheral subsystems are maliciously modified, the PUF cannot detect these changes since the PUF only protects the IC.

We address this system-level security gap by investigating the analog characteristics of circuit boards to determine if normal manufacturing process variation is sufficient to create unique hardware signatures which can distinguish between instances of the same PCB design. That is, the signature is unique to an individual PCB, rather than to a PCB model number. These unique signatures can be used directly for verifying the integrity and authenticity of the PCBs, or can serve as the basis for generating cryptographic keys for more secure authentication of the electronic device during system acquisition or field deployment. While such signatures have many applications, we focus our attention on using them for authenticating PCBs. Some of this work will extend IC-based PUF concepts to the PCB by exploring the use of dynamic responses of various wire trace patterns that can easily be designed into PCBs as an additional source of uniqueness. In addition, this work attempts to build unique signatures using commercial off the shelf (COTS) passive components, such as capacitors and resistors. If uniqueness can be derived using these techniques and existing design tools, then it might be possible to develop unique board level signatures without requiring system designers to utilize specialized or expensive manufacturing processes.

A. Background

Possible sources of variation in PCBs and discrete components can be identified by understanding the manufacturing processes in [6]-[10]. PCBs typically begin as a layered board: conductor foil, dielectric substrate, conductor foil. The foil and substrate are adhered with a heat and pressure lamination process. A circuit design file (e.g. Gerber)

Sandia National Laboratories is a multi-mission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA-0003525. SAND2017-XXXX

The author's affiliation with The MITRE Corporation is provided for identification purposes only, and is not intended to convey or imply MITRE's concurrence with, or support for, the positions, opinions, or viewpoints expressed by the author. Approved for Public Release Case No. 17-2559

978-1-5386-1585-0/17/$31.00 ©2017 IEEE

is then used to generate a print on a photo imageable resist film which is also applied by heat and pressure to the conductor layers. The board is exposed to high intensity UV light and then etched with a chemical solution to create the first layers of wire traces. Inner vias are then drilled and plated. Additional layers can be created by applying a dielectric preimpregnated bonding layer, additional foil and repeating the process until the final solder mask and tining of pads are completed. Current manufacturing processes allow for up to 40 conductive layers, a minimum 0.00275-in wire trace width, and 0.003-in spacing between wires. New processes allow COTS manufacturers to install buried chip resistors within the circuit board layers [7].

Similarly, there are multiple processes and materials in capacitor and resistor manufacturing which add to variations in device characteristics. Surface mount multilayer ceramic capacitors (MLC) utilize a printed electrode and ceramic sheet laminate process to create various capacitances [8]. Surface mount chip resistors are manufactured using several precision print steps with conductive and glass materials followed by heat treatment processes [9][10]. Intermediate steps use precision laser trimming or photolithography to create linear resistive characteristics of the resistors. The final components are then binned and marked 5%, 10%, or 20% tolerance based on the results of the manufacturing tests.

B. Research Objectives & Technical Challenges

The main objective is to find design patterns and techniques that system developers can use with their existing design and manufacturing processes to provide a robust authentication capability for electronic systems. The potential use of this research and technical approach is very broad. The proposed techniques use standard design tools and low-cost measurement approaches. The main technical challenge in this effort is to determine the feasibility of using wire trace patterns or discrete components for building unique signatures. The research must also identify efficient data collection and signature generation techniques. Likewise, the research must also determine which mathematical analysis techniques are best suited to transform raw measurements into unique signatures capable of establishing the authenticity of the PCBs. Additionally, we want to bound the sampling and analysis problem to one that can easily be implemented using COTS digital signal processors so that the techniques can be quickly and easily adopted.

Section II describes our approach and design of experiments. Section III describes how to use manufacturing variations in macroscopic structures of PCBs (wire traces) and discrete components to measure and combine different measurements to produce the output signature. Section IV highlights the practical use of these techniques and integration with existing technologies for determining system-level integrity and authenticity.

II. Approach

The experiment described in this research uses wide-tolerance surface-mount resistors and capacitors of various nominal values from several manufacturers. These components have been mounted on a PCB (Fig. 1) that also contains serial and

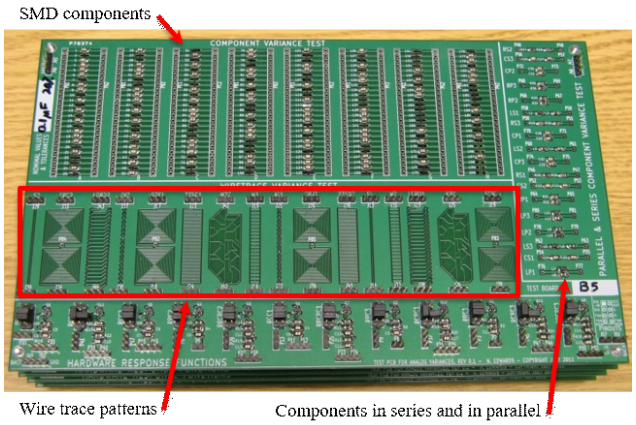

Fig. 1. Test board (1 of 10 shown).

parallel combinations of components. Wire trace patterns are placed across the mid-section of each board. We constructed 10 boards, each consisting of 100 discrete components, 9 instantiations of components in parallel, 9 instantiations of components in series, and 16 wire trace patterns. The boards are from a single batch run to emulate system manufacturing practices. If PCB uniqueness could be determined in a single batch (worst case for system variation), then the results from multiple batch runs are likely better. We will take measurements from our boards and then, by applying our past experience with PUFs, statistical test methodologies, and signal processing, establish techniques for generating reliable, unique signatures.

A. Design of Experiments – Wire Trace Signatures

For our experiments we considered measurements of 16 different wire trace patterns, which utilize 8 mil trace width spacing. Several of the patterns include multi-layer routing through the 0.064-inch FR4 circuit board. Within an environmentally controlled laboratory, we presented square wave inputs to each wire trace. We utilized LabView to orchestrate the tests and an advanced oscilloscope to capture the signal response data. To be consistent with typical analog signal sampling capabilities we vary the input frequency from 250kHz to 25MHz in steps of 250kHz. At each frequency we captured various properties of the output waveform including high and low voltage levels, overshoot, undershoot, 20% and 80% rise time and fall time, and rising and falling skew. The wire trace patterns we considered are shown in Fig. 1, with greater detail of a selection of them shown in Fig. 2. Each trace is identified by a name: Alternative Via (AV), Board-inductor (LBRD), Multi-Path (MP), Straight (S), Spiral with Follower-trace (SPF), Spiral with Via (SPV), Wide segments (W), Zig-zag square shape (ZZSQ).

B. Design of Experiments – Discrete Component Signatures

In this work, we consider measurements of discrete resistors and capacitors which can be measured in-situ (built-in to the system) or by an external device. In particular, we consider 0.01µF, 0.1µF, and 10µF capacitors and 1KΩ, 10KΩ, and100KΩ resistors. For each component value we have 33

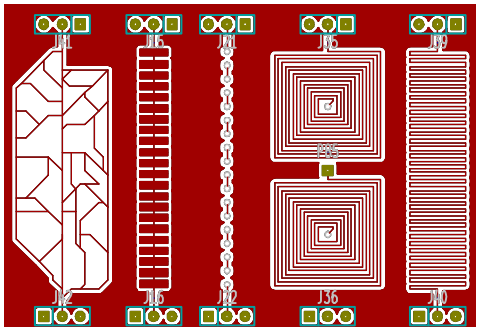

Fig. 2. A sample of different wire trace patterns studied. Several patterns include multi-layer routing, edge transitions, and vias.

individual devices from each of three manufacturers, resulting in 99 devices for each component value. The individual components were arbitrarily selected from various distributors to emulate manufacturing supply chain practices, and then were randomly placed on one of 200 test pads on each circuit board. We also consider series and parallel combinations of 0.1μF capacitors and of 10KΩ resistors. All of the individual components were randomly placed on one of 200 test pads on each circuit board.

We measured the component resistance or capacitance with a high resolution calibrated multimeter. The data collection was performed in a random order to eliminate experimental nuisance factors in the data. Details of generating and analyzing component signatures are described in Section III, while use of the signatures are described in Section IV.

III. Testing for Uniqueness– Analysis of Results

The quality of the bitstrings produced by PUFs are evaluated using several statistical metrics. Three particularly important criteria must be met for a PUF to be effective for encryption, random number generation, authentication, and so forth. First, the bitstrings must be *random* and unbiased, making them difficult for an adversary to model or predict. Second, the bitstrings produced from each board must be sufficiently *unique* (also called inter-device variation) to distinguish one board from every other board, and finally the bitstring for any one board must be *stable* (also referred to as intra-device variation) such that a reproduced bitstring is sufficiently close to the original [11]. We can evaluate bias as the sum of the bitstring divided by the length of the bitstring. The ideal bias is then 0.5. Inter-device variation is evaluated by XORing the bitstrings from two distinct PCBs and then summing the result and dividing the sum by the length of the bitstrings. The ideal inter-device variation is also 0.5. Intra-device variation is evaluated by XORing two measurements of the bitstring from a single PCB, summing the result, and then dividing the sum by the length of the bitstring. The ideal intra-device variation is zero.

In addition to these, tests that are more rigorous are defined in the NIST 800-22 test suite [12]. This test suite is a statistical package used for testing the randomness of (arbitrarily long) binary sequences produced by either hardware or software based pseudo-random number generators. This test suite consists of a set of 16 tests focusing on a variety of different types of non-randomness that could exist in a sequence. Some tests may be decomposed into a variety of sub-tests, therefore, a total of 189 items exist in the test suite. The 16 types of tests are described in more detail in the standard.

To generate signatures from a collection of n-measurements we place the first *n/2* measurements in one set, and the remaining *n/2* measurements in a second set. Then we compare each element from the first set to each element from the second, and output signature bit '1' if the value from set *A* is greater than that from set *B*, and a '0' otherwise. This results in an $(n/2)^2$-bit signature.

A. Signatures from Wire Trace Patterns

We have identified a variety of approaches for making comparisons between wire trace measurements. One possibility is to make comparisons between a single type of measurement across frequencies on a particular wire trace structure. For instance, we may compare the rise times at distinct frequencies f_1 and f_2, which we denote as Rf_1 and Rf_2. The most straight-forward approach is simply to produce output bit '1' if $Rf_1 > Rf_2$ and output bit '0' otherwise. Another possibility is to compare each rise time $Rf_1, Rf_2, \ldots, Rf_n$ to the mean, median, or some other population average of the rise times. Then, at each frequency $f_1, f_2, \ldots, f_n$ we can produce bit '1' if the rise time at that frequency was greater than the population mean and bit '0' otherwise. Then, rather than comparing the rise times themselves we can XOR pairs of these bits to produce the output bits. We can do the same with the fall times $Ff_1, Ff_2, \ldots, Ff_n$. and combine bits from these different sets with a binary function, such as the two-input XOR.

We can also make comparisons between different measurements at a fixed frequency. For example, for some fixed frequency f we can compare the rise time Rf_n to the fall time Ff_n and output bit '1' if $Rf_n > Ff_n$ and bit '0' otherwise. Since consistent, predictable bias may be present in comparisons such as this, we can instead convert the Rf_n and Ff_n to binary values by comparing them to their population averages, as described above, and then use binary functions to combine these values.

Finally, we can also combine the previous two approaches by comparing different measurements at different frequencies. For this, we should again normalize individual measurements by comparing them to their population averages, for example, by comparing each of the rise times $Rf_1, Rf_2, \ldots, Rf_n$ to the population average of rise times across all frequencies, and then generating bit '1' if an individual measurement is greater than the population average and bit '0' otherwise. After performing a similar calculation for each measurement type (i.e. high and low voltage levels, overshoot, undershoot, rise time and fall time, rising and falling skew) we can compare the different measurement types to each other across frequencies by combining the bits associated with the measurements with a binary function, such as the two-input XOR. We use this approach for the following results.

Our generated signatures pass all of the NIST 800-22 statistical tests for randomness and pseudo-randomness. Table I shows the inter-device Hamming distance results. Since one of the research goals is determine if any wire trace pattern is

not useful for unique signature generation we can eliminate the structures that have low inter-device Hamming distance (i.e. both instances of LBRD, SPF, SPV, ZZSQ patterns). Table I indicates that the high and low voltage "levels" measurement for test structures with wire trace patterns AV, MP, S, and W are the best performing when considering inter-device Hamming distance. Fig. 3 graphs the relationship between intra-device and inter-device Hamming distance for wire trace structure AV1 and shows close to ideal inter-device variation.

B. Signatures from Discrete Component Measurements

Fig. 4 reveals a clear, systematic variation in measured values across manufacturers which can create a signature generation bias. Although the data collection was performed in a statistically random order to eliminate experimental nuisance factors, the bias exists because, for example, measured values from the first manufacturer of 10µF capacitors are greater than all of the measured values from the second and third manufacturers. Due to this the measurements from the first manufacturer will tend to be above the population mean, introducing a bias into the output signature. The combination of series or parallel components have monotone characteristics (Fig. 5) which can also introduce bias into the generated signatures. Consequently, we cannot use the measured values directly for generating signatures, since this systematic bias will result in predictable signatures, which is undesirable.

As before, we can eliminate some of the bias by comparing each measurement to the mean or median of the full set of measurements for that component. We output a '1' if the value exceeds the mean or median and a '0' otherwise. To obtain a signature, we again divide the measurements into two sets. Then we XOR each element from the first set with each element from the second set. While this normalization is helpful, it does not result in complete elimination of the bias. To correct for this we permute the order of the measurements prior to forming the signature by randomly distributing the different manufacturers amongst our two sets which helps eliminate bias resulting from systematic variations between manufacturers. This eliminates almost all of the bias in the output signatures, as shown in Table II. The signatures are 2401 bits long for the capacitors and resistors, and 169 bits long for the series and parallel combinations.

Now, notice that since we have normalized data, we aren't restricted to comparing like elements to each other. Rather, we can compare the normalized responses. So, for example, we can combine bits from the 0.01uF capacitors with those from the series 10K resistors. This provides us with many more input bits, permitting much longer responses. To accomplish this, we concatenate all of the normalized responses, perform random assignment of values to the two sets, and then generate the device signature. This results in signatures with essentially no bias, full Shannon entropy, and almost full minimum entropy, as shown in Table III. In this case, the signatures are 123,201 bits long.

Finally, since we have three manufacturers for each type of resistor and capacitor we can extract signatures from the analog measurements of each type of component on a manufacturer by manufacturer basis. As before, we consider both mean and median normalization and randomly assign components to the two sets. This results in 256-bit signatures. Results for the median normalized capacitor data are shown in Table IV. Ultimately this shows the technique is still valuable for an electronic device production line is limited to one manufacturer of discrete component due to supply chain or value stream process constraints.

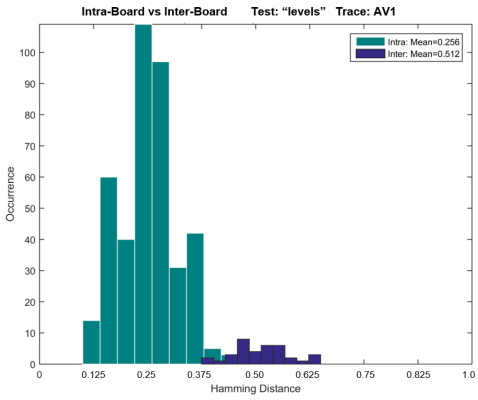

Fig. 3. Hamming distance distributions for Intra-device and Inter-device of wire trace pattern AV1 for voltage levels (high and low) measurement.

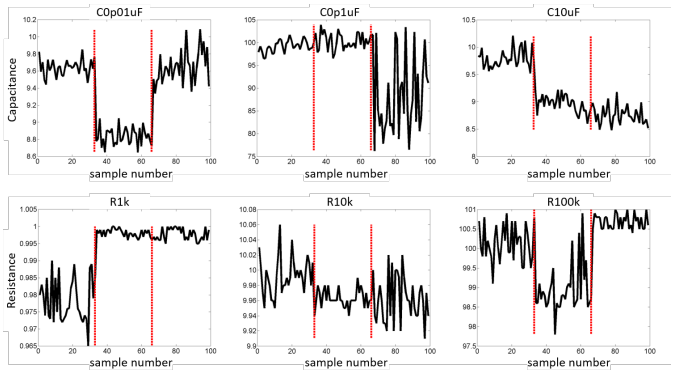

Fig. 4. Systematic variation in the measured values of surface mount capacitors (*top*) and resistors (*bottom*) from different manufacturers.

TABLE I. INTER-DEVICE HAMMING DISTANCE FOR EACH TRACE/TEST (UP TO 10MHZ). DATA USED IN FINAL SIGNATURES ARE GREEN

	16 Printed Circuit Board Test Structures															
	AV1	**AV2**	**LBRD1**	**LBRD2**	**MP1**	**MP2**	**S1**	**S2**	**SPF1**	**SPF2**	**SPV1**	**SPV2**	**W1**	**W2**	**ZZSQ1**	**ZZSQ2**
Fall Time	0.3542	0.3333	0.2278	0.2139	0.3639	0.3069	0.3556	0.3444	0.1986	0.2361	0.0236	0.0292	0.3389	0.3250	0.3458	0.3250
Levels	0.5125	0.4736	0.1639	0.1931	0.4917	0.5056	0.5042	0.5000	0.2597	0.2750	0.2361	0.3486	0.4944	0.4667	0.4875	0.4958
Overshoot	0.0431	0.0333	0.0236	0.0111	0.0472	0.0583	0.0194	0.0319	0.0181	0.0375	0.0708	0.0681	0.0264	0.0250	0.0417	0.0431
Rise Time	0.3333	0.3542	0.3014	0.2597	0.3514	0.3278	0.3917	0.3750	0.2278	0.2111	0.0139	0.0139	0.3236	0.3347	0.3847	0.3667
Undershoot	0.0778	0.0764	0.0569	0.0486	0.0986	0.1028	0.0708	0.0542	0.0417	0.0347	0.0250	0.0403	0.0972	0.0778	0.0847	0.0736
Skew	0.3208	0.3097	0.1972	0.2000	0.3292	0.3847	0.3958	0.2889	0.1056	0.1167	0.0917	0.0500	0.3750	0.3806	0.2528	0.1889

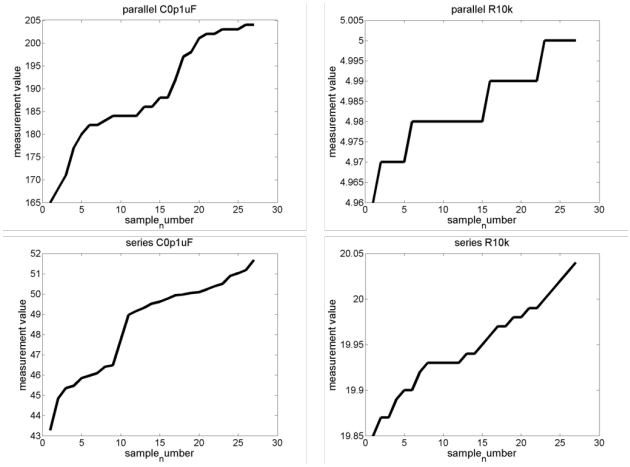

Fig. 5. The parallel and series combinations of components are monotonically increasing.

IV. Practical Use of Wire Traces And Discrete Components for Systems

At this point we have established our ability to extract PCB specific, random signatures from wire trace structures or discrete components. We now turn our attention to a brief discussion on using these measurements to authenticate PCBs. One method of authentication involves challenge-response pairs. A single challenge signal is selected and the response from wire traces or discrete components are measured. Then, this new response is compared to the response stored in secure memory and, if they are close enough to each other, then the device is deemed authentic. To define a challenge, the system can use a specific set of traces where measurements on those traces are the challenge. A second approach is to fix a specific set of measurements, and to use the traces involved in those measurements as the challenge. A third approach is to fix the traces, and to define the set of measurements as a challenge. To implement this, we can have either an on-board measurement device or an external measurement device for capturing the device signature. The same approaches can be applied to a set of discrete components with its measurements and responses. Other approaches may also be possible. For instance, the challenge may be generated using some external stimulus, such as a password or biometric. This would allow the challenges and responses to be specific to individual users.

Another use of this research is to generate a single response signature as previously described, and then use it to derive a cryptographic key or key pair for use in a cryptographic authentication scheme. This method requires fixing a challenge so that a specific response can be reliably generated. Fuzzy extraction and other data processing techniques may be required to ensure reliable key generation [13].

Now, we consider several methods for combining our wire trace and discrete component signatures, called a board signature, with other existing signature technologies. One concept is to incorporate the IC PUF signature as a third input

TABLE II. Elimination of Signature Bias using Permuted Measurements

Components	*Original Bias*	*Permuted, Mean Normalized*	*Permuted, Median Normalized*
0.01µF	0.49	0.46	0.53
0.1µF	0.67	0.40	0.51
10µF	0.95	0.47	0.50
1KΩ	0.20	0.45	0.48
10KΩ	0.66	0.49	0.49
100KΩ	0.29	0.49	0.50
Parallel 0.1µF	0	0.49	0.57
Parallel 10KΩ	0	0.60	0.60
Series 0.1µF	0	0.47	0.50
Series 10KΩ	0	0.50	0.52
Parallel 0.1µF	0	0.49	0.57

TABLE III. Permuted Measurements, Component Types Concatenated

	Mean Normalized	*Median Normalized*
Bias	0.4936	0.4973
Entropy	0.9999	1.0000
Min Entropy	0.9816	0.9923

TABLE IV. Individual Manufacturer signatures, Median Normalized, Random Set Assignments

Capacitors			
Values	**Bias**	**Entropy**	**Min Entropy**
0.01µF (mfg. 1)	0.50	1	1
0.01µF (mfg. 2)	0.50	1	1
0.01µF (mfg. 3)	0.52	0.9993	0.9556
0.1µF (mfg. 1)	0.57	0.9857	0.8102
0.1µF (mfg. 2)	0.50	1	1
0.1µF (mfg. 3)	0.53	0.9972	0.9125
10µF (mfg. 1)	0.55	0.9937	0.8707
10µF (mfg. 2)	0.50	1	1
10µF (mfg. 3)	0.51	0.9998	0.9776
Resistors			
Value	**Bias**	**Entropy**	**Min Entropy**
1kΩ (mfg. 1)	0.55	0.9937	0.8707
1kΩ (mfg. 2)	0.52	0.9993	0.9556
1kΩ (mfg. 3)	0.50	1	1
10kΩ (mfg. 1)	0.48	0.9984	0.9339
10kΩ (mfg. 2)	0.45	0.9937	0.8707
10kΩ (mfg. 3)	0.48	0.9993	0.9556
100kΩ (mfg. 1)	0.52	0.9984	0.9339
100kΩ (mfg. 2)	0.55	0.9937	0.8707
100kΩ (mfg. 3)	0.50	1	1

along with discrete components and wire traces. The "normalization" method is used to generate a stream of bits from an IC PUF, and then combined with the board signatures using techniques described in Section III. Another option is to concatenate the board signature with the IC PUF signature. A third option is to use the board signature to select a challenge

for the IC PUF, or to use the IC PUF to select a challenge for the board signature. Note that the IC PUF is not explicitly required; wire trace and discrete component signatures can be used independently to authenticate and verify the integrity of PCBs. We also note that combined signatures can additionally be coupled with some external factors such as a user's password or biometric to create a signature that is unique to the combination of user and PCB. Several approaches for this have been described previously [14].

Another important use of this technology is to help identify and deter counterfeit electronics. For counterfeit mitigation the PCB manufacturer can measure the PCB signature or establish an asymmetric key pair from the signature, and associate it with the PCB's serial number. Later, the consumer of the PCB can measure the signature or regenerate the key pair from the signature and verify this against the manufacturer's database. Counterfeit PCBs will not appear in that database unless the counterfeiter also gains access to the database [15]. Furthermore, these methods of using discrete components and circuit board wire traces add complexity for an attacker. While it might be possible to record the board-level PUF responses and replay with a signal generator, such an attack would take much time to understand which wire traces or components are used to generate the board level signature. Additional obfuscation and thus increased complexity is gained by using existing functional subsystem board designs (wire traces and components), randomly ordered input signals, or random sampling times. Incorporating an IC PUF for a system-level signature increases the attacker's cost in time and resources. Finally, due to the intrinsically unique properties of our approach, the signature can be used to identify specific PCB and electronic devices in the case that it is observed in use after being officially decommissioned. Our work demonstrates that it is not probable to replicate or counterfeit a circuit board with the same signature using current manufacturing technology.

V. Summary

With our novel approaches we successfully generated unique identifiers for PCBs from manufacturing variations in the electrical characteristics of surface mount resistors and capacitors, and from the dynamic characteristics of signal responses in PCB wire trace test structures. We presented an approach for generating the unique identifiers using a normalization approach that compares each measurement in a population to some population average (e.g. mean or median) producing bit '1' if the measurement is greater than the average and bit '0' otherwise. Concatenating the different component types, normalizing, and permuting the order of measurements (normalizing) eliminates most of the bias in the responses and results in signatures with nearly ideal statistical properties.

We also described several approaches for combining wire trace and discrete component signatures, with an IC PUF signature or other external factors. These unique signatures can be used directly for verifying the integrity and authenticity of the PCBs, or can serve as the basis for generating cryptographic keys. Our results indicate that the proposed approaches for measuring and combining these quantities are capable of generating high-entropy, unique signatures for PCBs. The techniques explored do not require system designers to utilize specialized manufacturing processes and implementation is low-cost.

Future work in this area would include specific experiments which identify ideal wire trace pattern characteristics such as shape, trace length, trace width, circuit board dielectric thickness, or other. Research is also needed to optimize the measured entropy and uniqueness by understanding the correlation between ideal wire trace patterns and sampling frequencies. Future research should also include environmental or aging effects on the signatures, and may also reveal new concepts to combine multiple sampling techniques and physical structures.

Acknowledgment

This research is covered under pending U.S. Patent Application No. 15/624,907 [16].

References

[1] L. Greenemeier, "The Pentagon's seek-and-destroy mission for counterfeit electronics," *Scientific American*, Apr 28, 2017.

[2] J.R. Hamlet, T.M. Bauer, and L. Pierson "Modelling-Resistant Physical Unclonable Functions," *Annual Computer Security Applications Conference*, Sandia National Laboratories, 2014

[3] J.R. Hamlet, D.J. Stein, and T.M. Bauer. "Hardware device to physical structure binding and authentication." U.S. Patent No. 8,516,269. Aug 20, 2013.

[4] J. Zhang, et al. "A PUF FSM binding scheme for FPGA IP protection and pay-per-device licensing." *IEEE Trans. Inf. Forens. Security* pp1137-1150, 2015

[5] F. Koushanfar,. "Integrated circuits metering for piracy protection and digital rights management: an overview," in *Proceedings of the 21st Edition of the Great Lakes Symposium on Great Lakes Symposium on VLSI*, New York, NY, 2011, pp. 449–454.

[6] Advmaced Circuits Inc., *Building a printed circuit board*, 2009

[7] Advanced Circuits Inc., *Printed Circuit Boards Manufacturing & Assembly Capabilities*, [Online].: http://www.4pcb.com/expanded-capabilities.html. [Accessed: 19-Jun-2017].

[8] John Piper, ""Wet Vs. Dry" Multilayer Ceramic Capacitor Manufacturing Processes," KEMET Tech Topics, vol. 1, Aug 4, 1991.

[9] Michael Randall, "The Definitive Guide to SMT Resistor Selection," Venkel Ltd., White Paper.

[10] R-Chip PM Team, "Yageo Chip - Resistor Introduction," Apr-2012.

[11] Meng-Day Yu, et al. "Performance metrics and empirical results of a PUF cryptographic key generation ASIC." *Hardware-Oriented Security and Trust (HOST), 2012 IEEE International Symposium on*. IEEE, 2012.

[12] *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*, NIST Special Publication 800-22, rev 1A, April 2010

[13] Y. Dodis et al., "Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data," *SIAM J. Computing*, vol. 38, no. 1, 2008, pp. 97–139.

[14] T. Bauer, R. Birmingham, and J.R. Hamlet. "Circuit that Includes a Physically Unclonable Function." U.S. Patent Application No. 15/077,488. Filed 22 March, 2016.

[15] J.R. Hamlet, T.M. Bauer, and L.G. Pierson. "Deterrence of device counterfeiting, cloning, and subversion by substitution using hardware fingerprinting." U.S. Patent No. 8,848,905. 30 Sep. 2014.

[16] N.J. Edwards, J.R. Hamlet, and M.T. Martin, "Authenticating a Printed Circuit Board." U.S. Patent Application No. 15/624,907. Filed 16 June, 2017.