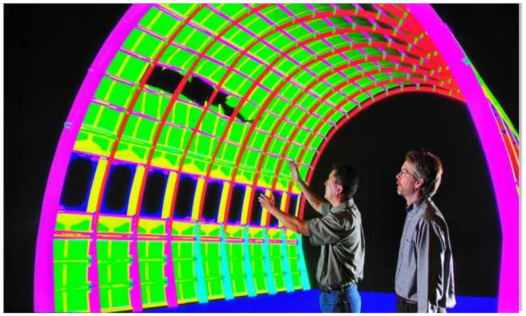
ICCST–2017
51st International Carnahan Conference on Security Technology, Madrid, Spain

SAND2018-1455C



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

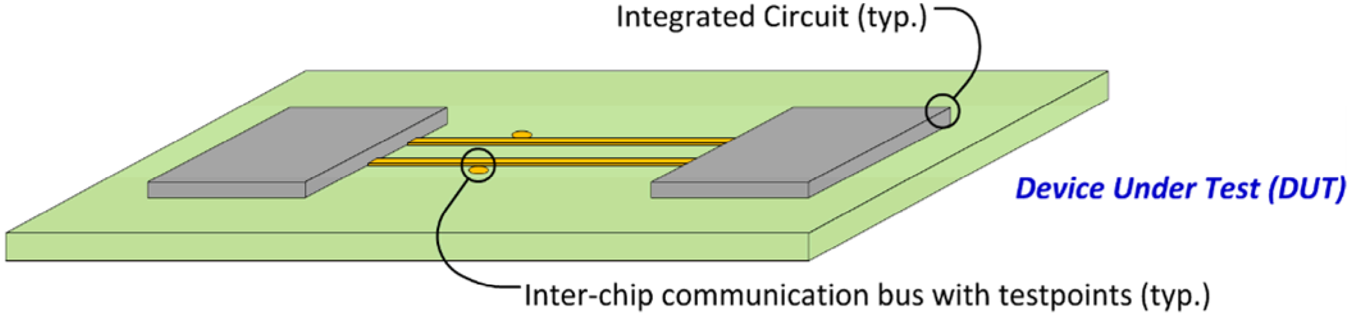
Nathan Edwards, *The MITRE Corporation*
Jason Hamlet, *Sandia National Laboratories*
Mitchell Martin, *Sandia National Laboratories*

U.S. Patent Pending 15/624,907 “Authenticating a Printed Circuit Board”

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & 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-NA0003525.

Research Gap

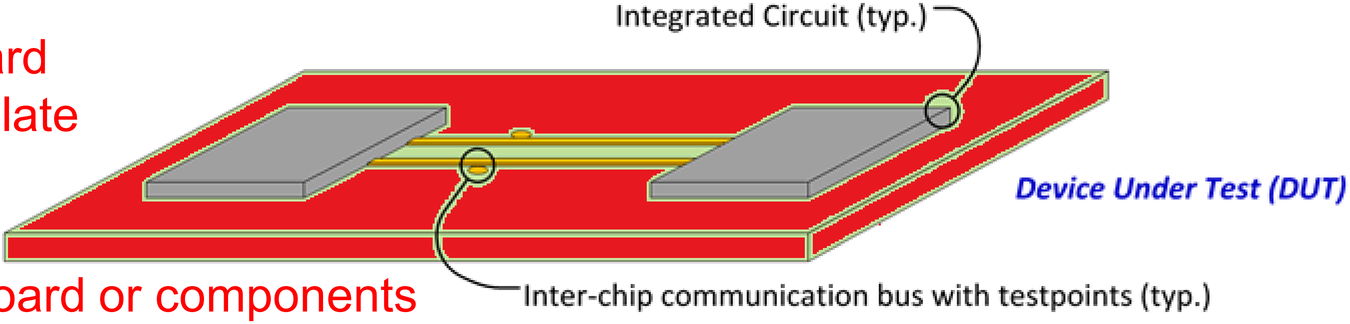
- Globalization in supply chains of electronics has increased concerns of counterfeits and malicious modifications
- Challenge is how to detect & prevent tampering and counterfeiting, and determine electrical system authenticity
- Current manufacturing tests do not account for authenticity
- Existing work and mitigations:
  - Silicon-based Physical Unclonable Functions (PUF)
  - Tamper prevention/detection enclosures
  - Cryptographic algorithms (hardware/software)
- Gap: approaches do not address the whole electronic system


Integrated Circuit (typ.)
Device Under Test (DUT)
Inter-chip communication bus with testpoints (typ.)

Research Gap

- Globalization in supply chains of electronics has increased concerns of counterfeits and malicious modifications
- Challenge is how to detect & prevent tampering and counterfeiting, and determine electrical system authenticity
- Current manufacturing tests do not account for authenticity
- Existing work and mitigations:
  - Silicon-based Physical Unclonable Functions (PUF)
  - Tamper prevention/detection enclosures
  - Cryptographic algorithms (hardware/software)
- Gap: approaches do not address the whole electronic system

Malicious circuit board with ability to manipulate data, control, system

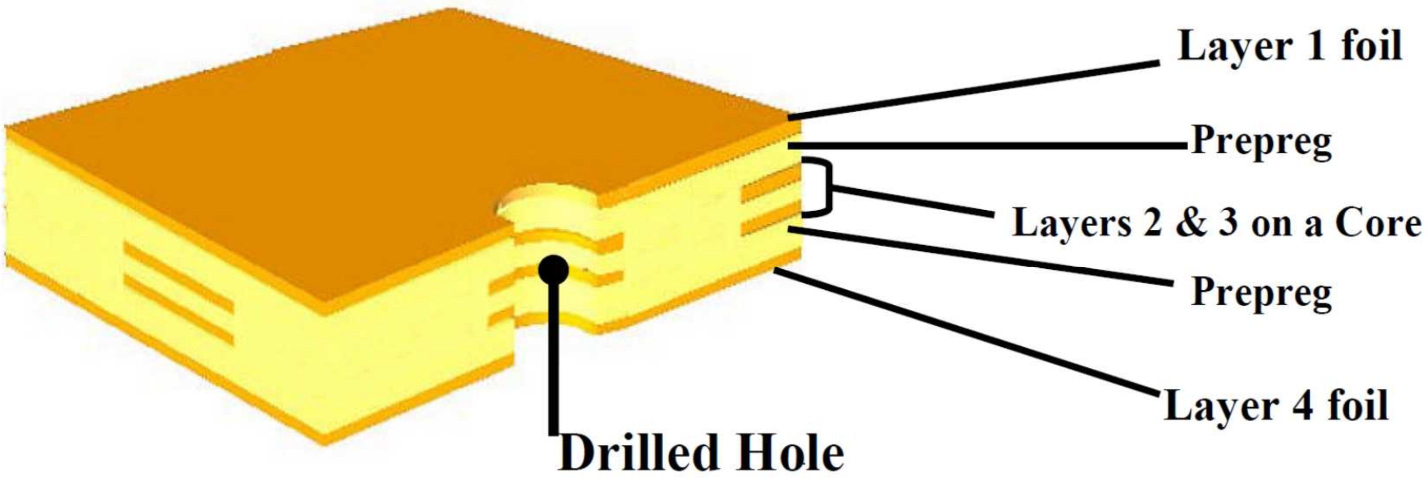

Integrated Circuit (typ.)
Device Under Test (DUT)
Inter-chip communication bus with testpoints (typ.)

Counterfeit circuit board or components

Our Approach

- Determine feasibility of using:
  - Printed circuit board wire trace design patterns for unique signatures
  - Discrete surface mount passive components for unique signatures
- Leverage existing design tools and manufacturing processes
- Identify low-cost sampling and signature generation techniques
- Bound the sampling and analysis problem to COTS components and techniques that can be quickly/easily adopted

Sources of Variation – Circuit Boards

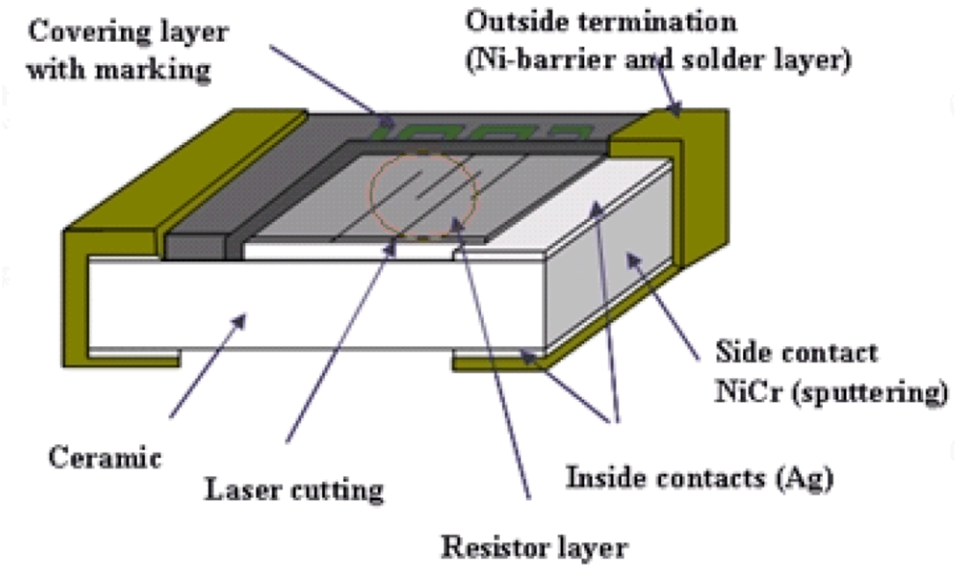


http://www.4pcb.com/media/building-printed-circuit-board.pdf

- Photoresist & Printing resolution
- Etching
- Dielectric layers
- Machining (drilled holes)
- Plating

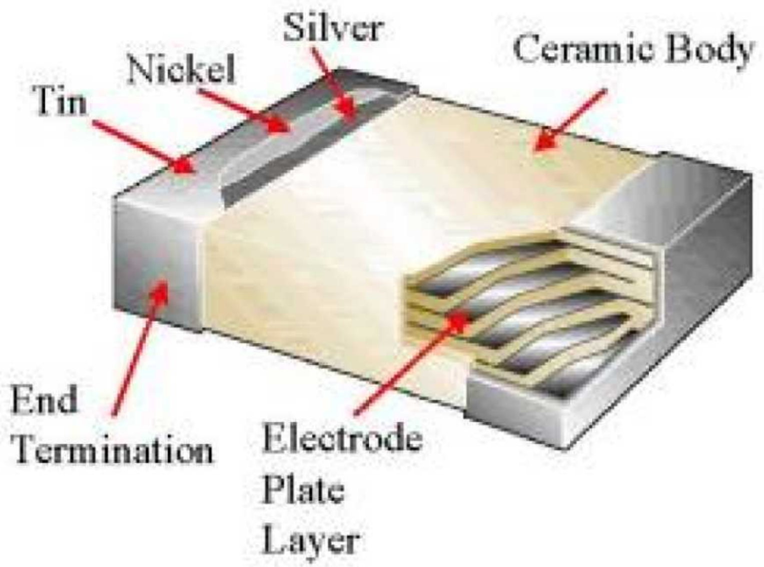
Sources of Variation – Passives

Thin Film Resistor


Covering layer with marking
Outside termination (Ni-barrier and solder layer)
Side contact NiCr (sputtering)
Ceramic
Laser cutting
Inside contacts (Ag)
Resistor layer

http://www.mouser.com/pdfDocs/Yageo_R-Chip_Resistor.pdf

Multilayer Ceramic Chip Capacitor

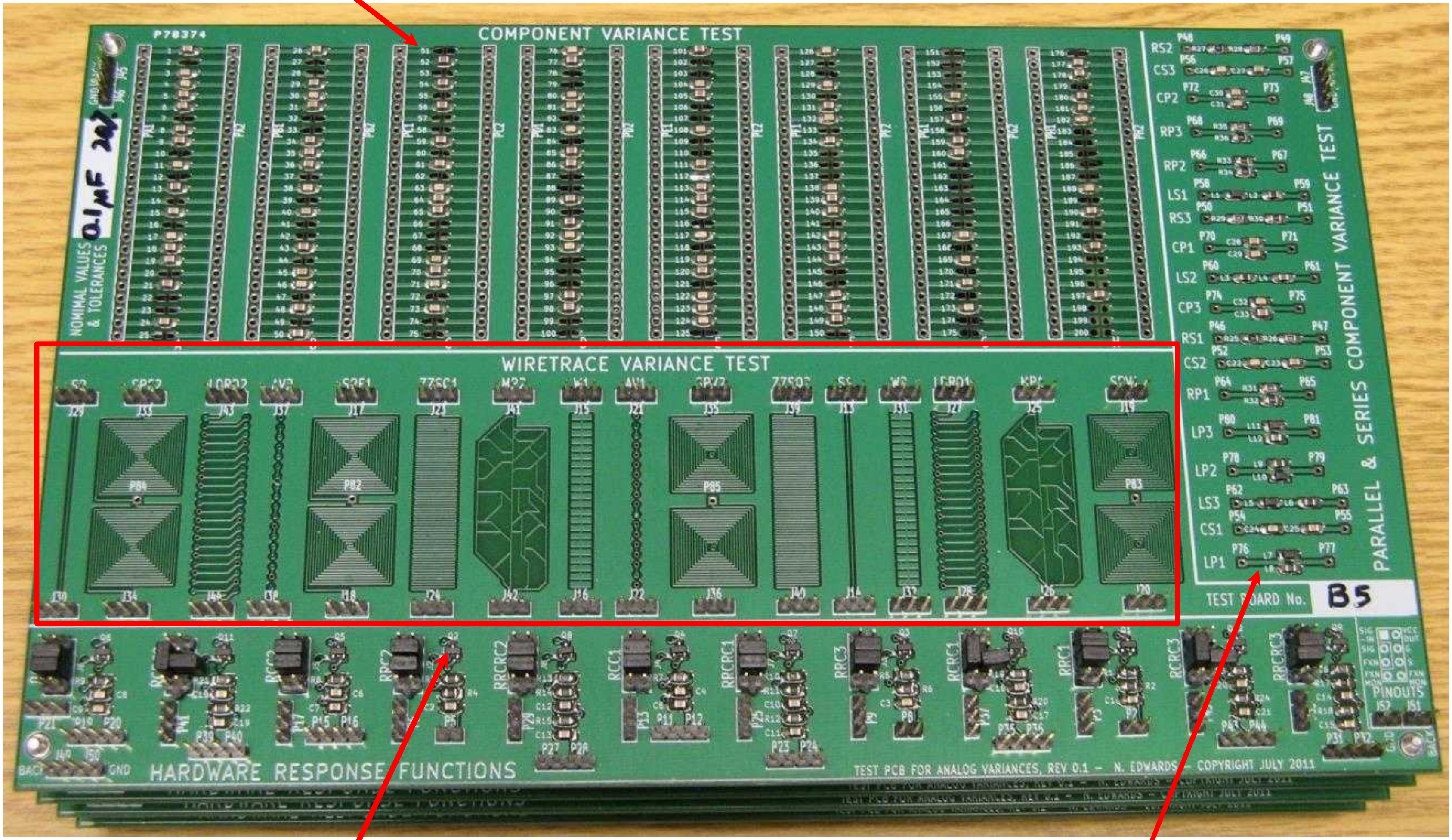


http://www.kemet.com/Lists/TechnicalArticles/Attachments/110/TechTopics%20Vol1No4%20Aug91.PDF

- Ceramic build-up
- Thermal fusing process
- Laser cutting
- Plating

Test Boards & Components

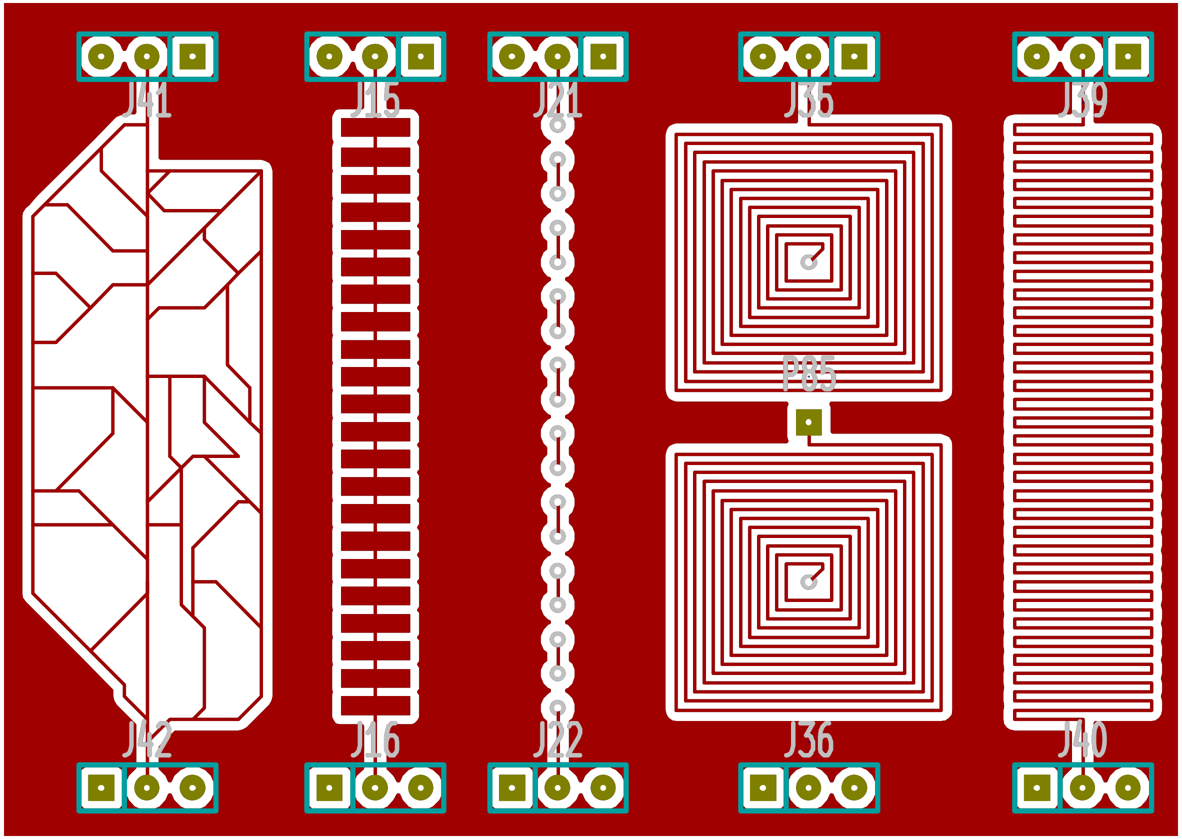
SMD components


P78374
COMPONENT VARIANCE TEST
NOMINAL VALUES & TOLERANCES
0.1µF 2k
WIRETRACE VARIANCE TEST
PARALLEL & SERIES COMPONENT VARIANCE TEST
TEST BOARD No. B5
HARDWARE RESPONSE FUNCTIONS
TEST PCB FOR ANALOG VARIANCES, REV 0.1 – N. EDWARDS – COPYRIGHT JULY 2011

Wire trace patterns

Components in series and in parallel

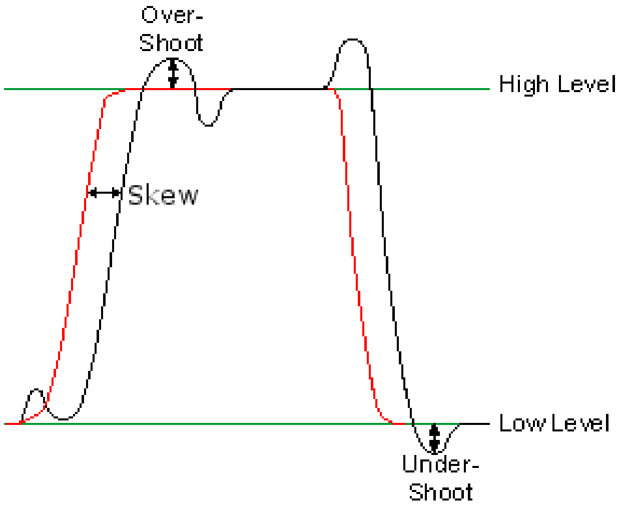
Examples of Wire Trace Design Patterns

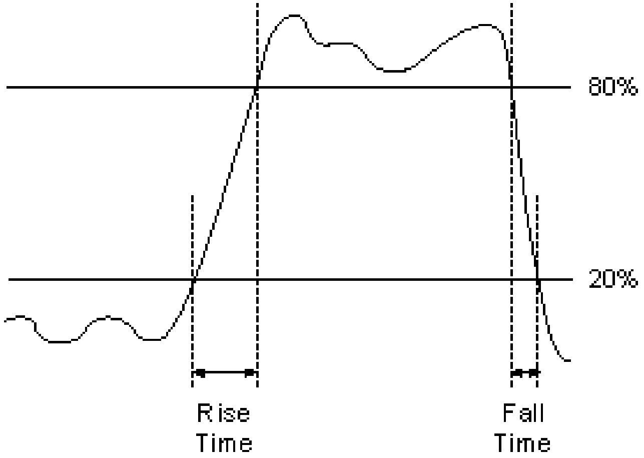


- Several patterns include multi-layer routing

Design of Experiments

- 10 test boards, each had:
  - 16 wiretrace patterns (8 designs)
  - 100 discrete components
  - 9 pairs of components in series
  - 9 pairs of components in parallel
- Component values measured with DMM
- Wire traces: 250kHz steps (0 – 25MHz)
- Measurements:
  - Levels (high and low)
  - Overshoot
  - Rise time
  - Undershoot
  - Skew (rising and falling)

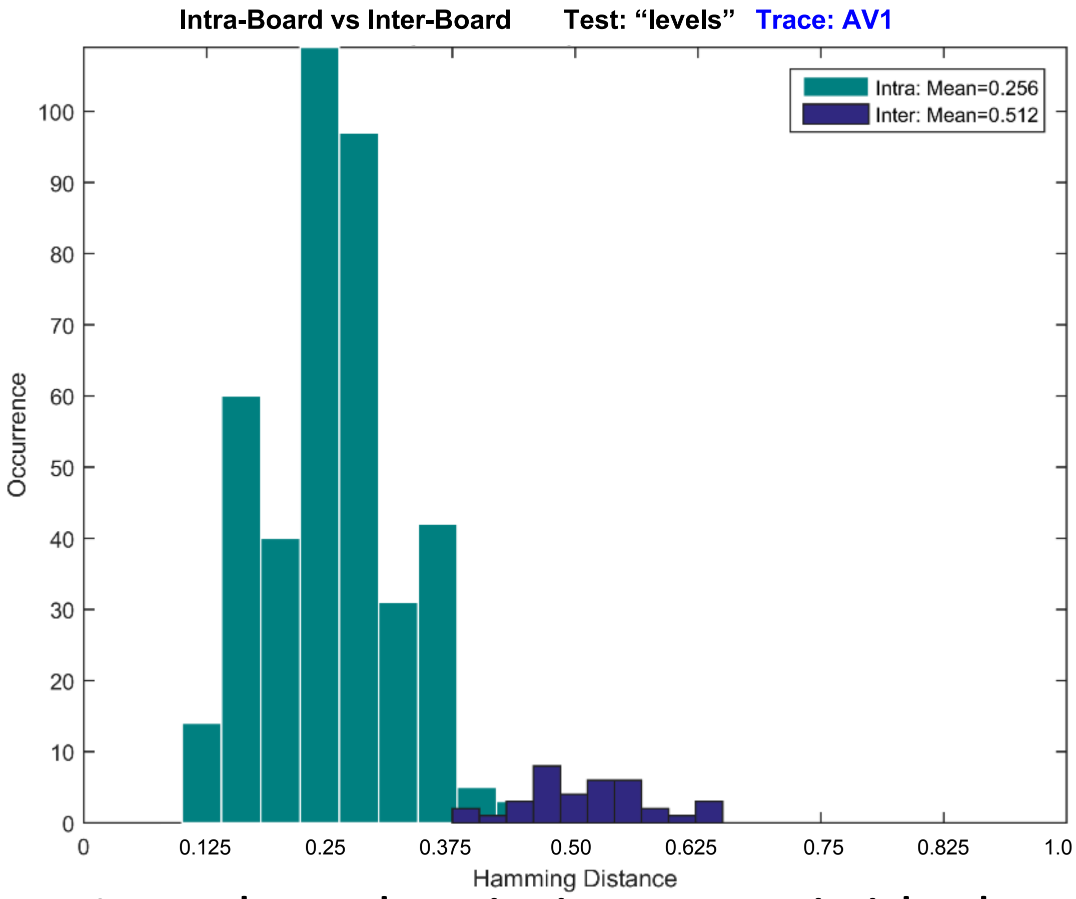




Building Signatures

- From a collection of n-measurements:
  - The first n/2 measurements are placed in one set
  - Remaining n/2 measurements in a second set
- Compare each element between sets:
  - ‘1’ if the value from set A is greater than that from set B
  - ‘0’ otherwise.
- Results in an $(n/2)^2$ bit signature
  - Applies to combination of manufacturers or within same mfg/lot
- Normalize by comparing each measurement to the mean or median of the full set of measurements for that component
- To obtain a signature:
  - Divide the measurements into two sets (A and B)
  - Then XOR each element in A with each element in B
- Can combine wire trace, component or other measurements

Wire Trace Variation Results



- Intra-board variation - zero is ideal
- Inter-board variation - 50% is ideal

- More traces or tests would increase bitstring size
- Passed all NIST statistical suite for Random and Pseudo Randomness (NIST SP800-22, rev 1A)

Overlap between intra- and inter-board variation creates a possibility of signature aliasing between distinct boards

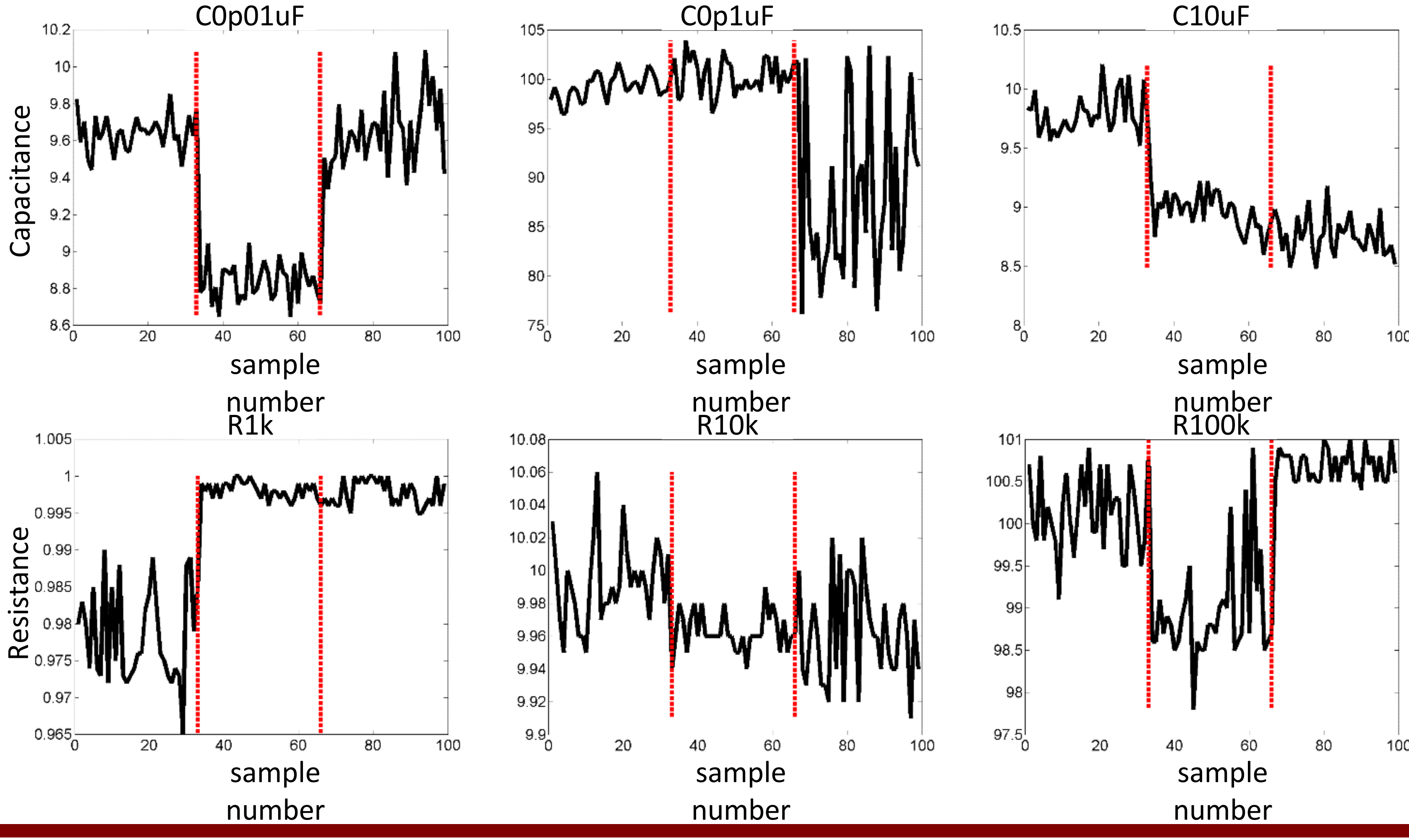
Wire Trace Variation Results

- Inter-board Hamming Distance for each trace/test (up to 10MHz)
- Design patterns have promising results: near 0.5 in some measurements
- Optimization problem exists:
  - selection of sampling frequencies, measurement types, design pattern, etc.
- Data used in final signatures are highlighted in 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

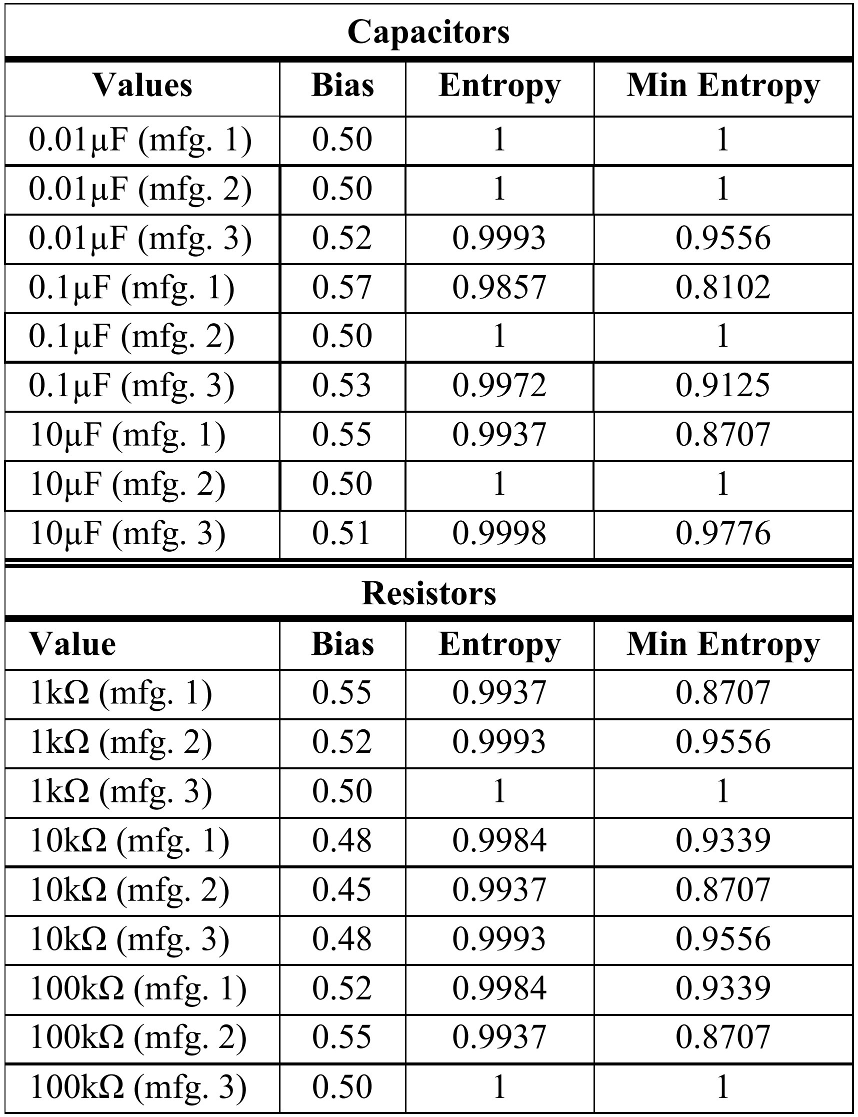
Passive Components

- Raw measurement of different manufacturers indicates that process variation of capacitors and resistors might be useful



Passive Component Results

- Individual manufacturer signatures, median normalized, random set assignments
- High entropy after normalization
- Combining measurements of different component types and values produces longer signatures



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

Summary and Applications

- Successful at constructing unique signatures with printed circuit board wire trace patterns and passive components
- Existing design tools and COTS components can be used

Applications:

- Hardware built-in testing & integrity measurements
- Advanced watermarking to identify electronic system counterfeits
- Basis for challenge-response authentication
- Signature can seed cryptographic key generation
- Ties device security technologies together at system level

Future Work

- Exploitation of environmental effects on signature variations
  - Passives are extremely susceptible to effects
  - Utilize environment for uniqueness of installation location
- Optimize the measurements per feature:
  - Sampling frequencies, measurement type, design pattern, etc.
- Abstract the best characteristics to provide design guidance to industry