# An Investigation into a Circuit Based Supply Chain Analyzer for FPGAs

FPL-2016

9/1/2016


Jacob Couch[1]

John Arkorian

Staff Researchers

[1]jacob.couch@jhuapl.edu

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

# What is the problem anyways?

- How can FPGAs be protected from supply chain vulnerabilities?
- Counterfeit and mislabeled FPGAs make their way into trusted systems.
  - Early failure rates
  - Subgrade performance
  - Unintended functionality

# But has this actually happened?

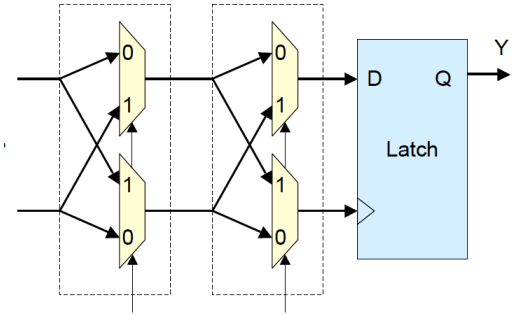
- **Examples [1]**
  - **USN P-8A Ice Detection System (FPGA)**
  - **USN SH-60B Forward Looking InfraRed (ASIC)**
  - **USAF C-130J Pilot Display System (ASIC)**



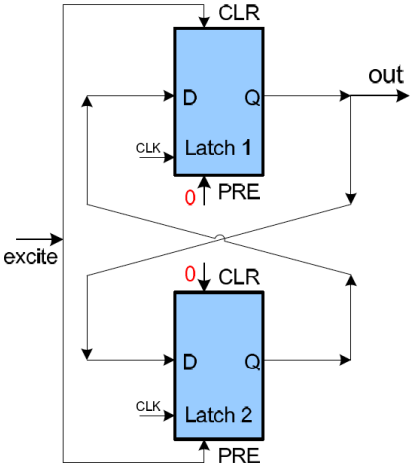

[1] J. Villasenor and T. Mohammad, “The Hidden Dangers of Chop-Shop Electronics,“ IEEE Spectrum, 2013.

# But we already have PUFs for this…

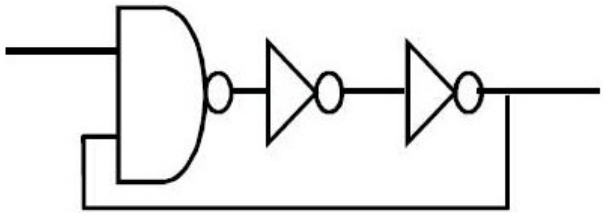
- **Physically Unclonable Functions provide a mechanism to *uniquely* identify a specific die through a set of challenges with *a priori* knowledge.**
- **These challenges provide either a 1 or 0 whose goal is to be stable across many different environmental conditions.**




Arbiter PUF [3]




Butterfly PUF [4]



Ring Oscillator PUF [5]


[3] A. Maiti and P. Schaumont, “Improved Ring Oscillator PUF: An FPGA-friendly Secure Primitive," Journal of Cryptology, vol. 24, no. 2, pp. 375-397, Oct. 2010.
[4] S. S. Kumar, J. Guajardo, R. Maes, G.-J. Schrijen, and P. Tuyls, “The buttery PUF protecting IP on every FPGA," in 2008 IEEE HOST. IEEE, Jun. 2008, pp. 67-70.
[5] G. E. Suh and S. Devadas, “Physical unclonable functions for device authentication and secret key generation," in 2007 DAC, p. 9.

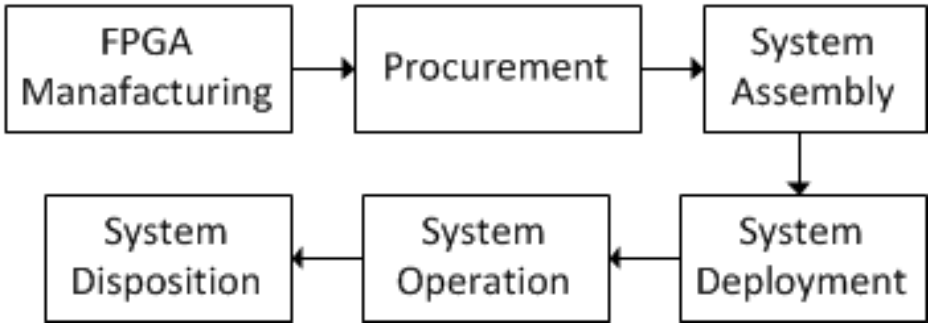
# But I always buy trusted new FPGA designs…

- **Many critical systems are still in limited production.**
  - **FPGA code can't be easily ported to a new platform without a recompilation.**
  - **This may trigger a new round of verification for the product to remain certified.**
  - **The economic case doesn't exist to recertify this product on a new FPGA.**
- **Counterfeit products are estimated to affect the global economy by over 1 trillion dollars.**
- **Counterfeit electronics are estimated to have a $169 billion impact.**
- **Counterfeit programmable logic is estimated to have a $2 billion impact. [6]**

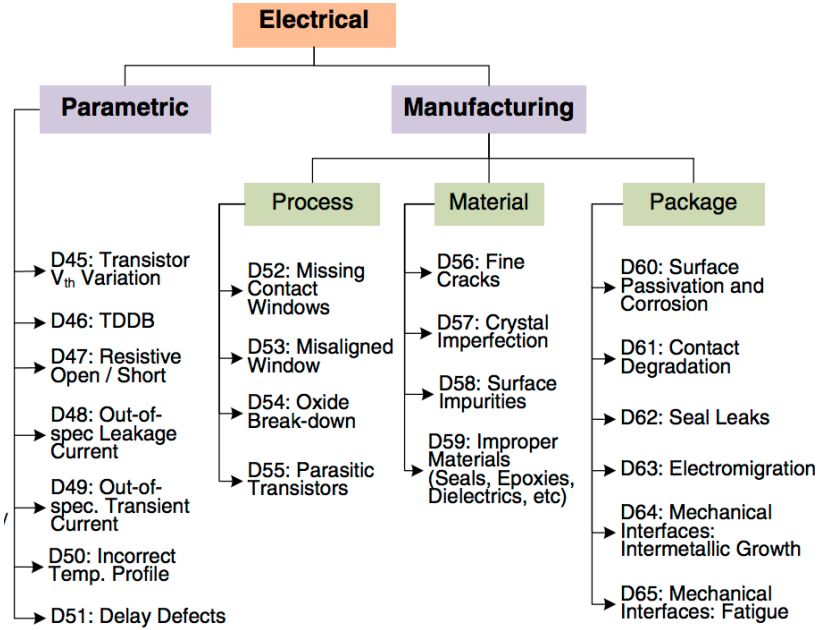

[6] IHS, "Top 5 Most Counterfeited Parts Represent a $169 Billion Potential Challenge for Global Semiconductor Market," 2012.

# Why should I care about counterfeit parts?

- **FPGA based systems have a long lifetime.**
- **Current methods of Supply Chain Management rely on initial verification procedures for parts.**




[7]



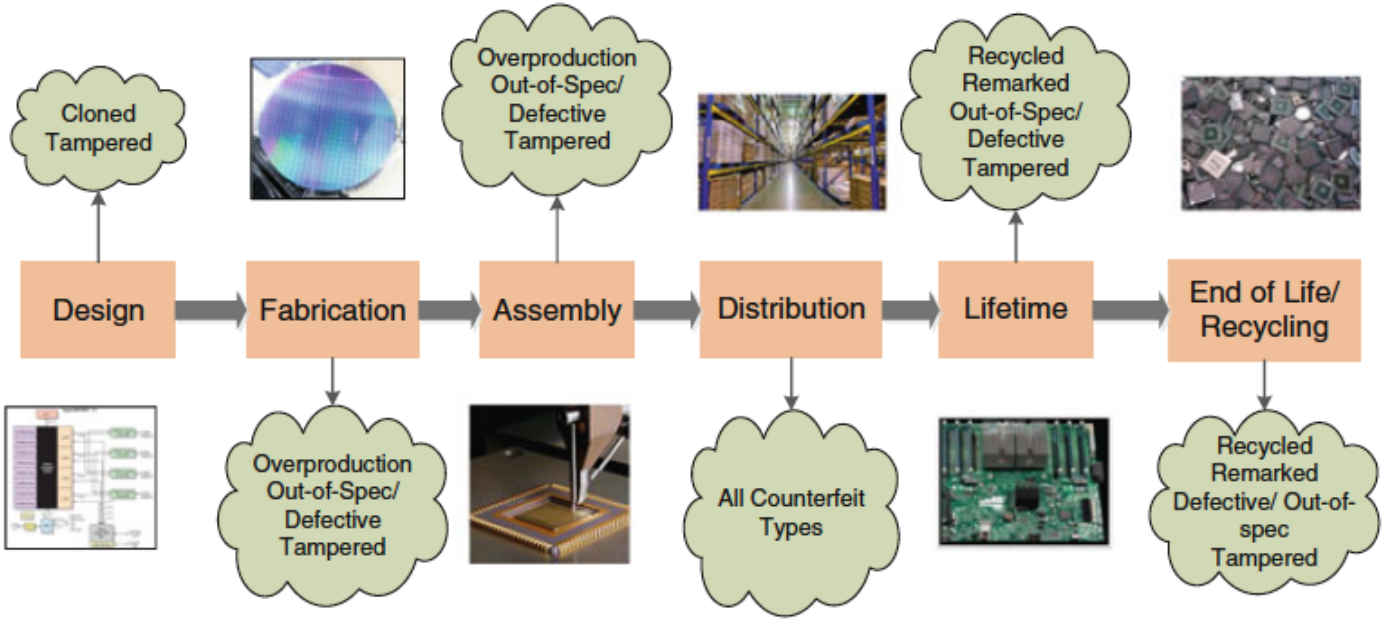

[8]


[7] S. Drimer, “Volatile FPGA design security a survey.”

[8] M. Tehranipoor, U. Guin, and D. Forte, “Counterfeit Integrated Circuits”. Springer International Publishing, 2015.

# Where can I be attacked?

- **Multiple attack vectors that cannot always be protected by policy and procedures.**




[9]

[9] U. Guin, D. DiMase, and M. Tehranipoor, "Counterfeit Integrated Circuits: Detection, Avoidance, and the Challenges Ahead," Journal of Electronic Testing, vol. 30, no. 1, pp. 9-23, Feb. 2014.

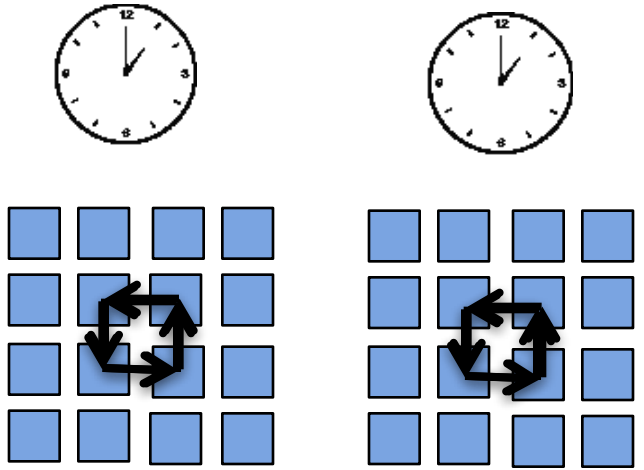
# Hasn't this already been done before?

- **Comparison of existing techniques by extending existing research.**

| IDs | Reliability | Uniqueness | Unclonable | Manufacturability | Cost effectiveness | Ease-of-Use |
|---|---|---|---|---|---|---|
| QR codes (Physical Artifact) | Not verified | Medium | Medium | Not verified | Not verified | High |
| DNA markings | Low | Low | Low | Low | Low | Medium |
| Nanorods (Physical Artifact) | Not verified | High | High | Not verified | Not verified | Medium |
| Physically Uncloneable Functions | Not verified | High | High | Not verified | Not verified | Medium |
| Scanning Electron Microscope | High | N/A | N/A | N/A | Low | High |
| Chemical Analysis | Medium Low | Low | Low | High | Low | Low |
| Foundry Identification[36] | Medium Low | Low | Low | N/A | Medium | Medium High |
| Recycled FPGA Detection[35] | Medium Low | Medium Low | Medium | N/A | Medium | Medium High |

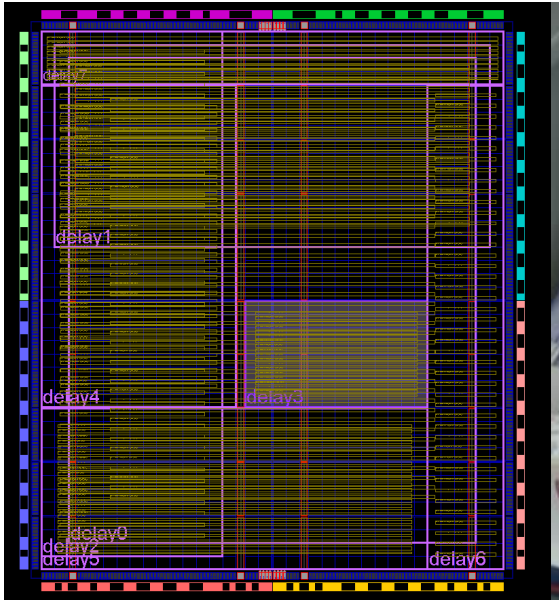
# How does this work?

- Multiple large ring oscillators are placed across the FPGA.
- They are measured against an external clock source.
  - This is in contrast to existing PUF implementations where a scalar value is generated for each measurement. Not a binary result.
- Goal is to detect inter lot variation and die aging variation.



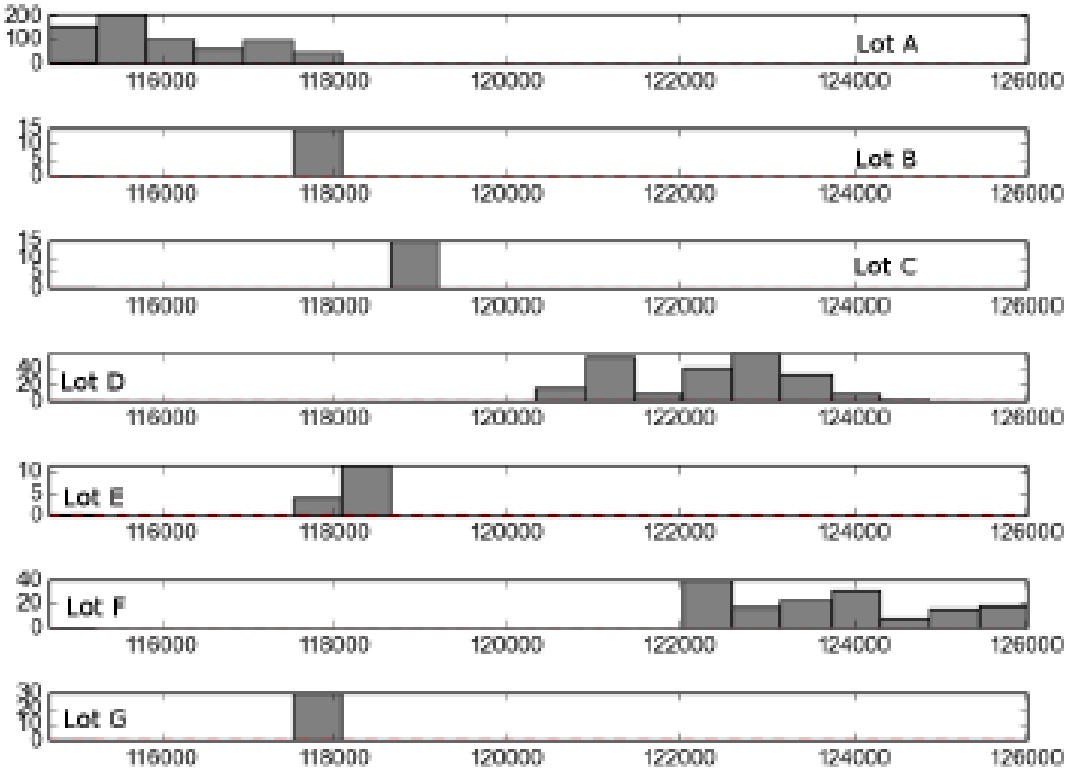
# How does this work?

- The 8 ring oscillators(ROs) were broken into the following lengths:
  - 4x256, 2x512, 2x1024.
- Two of the 256 ROs were constrained to the edges of the FPGA.
- Ring oscillators were constrained to 15-100% of the FPGA.



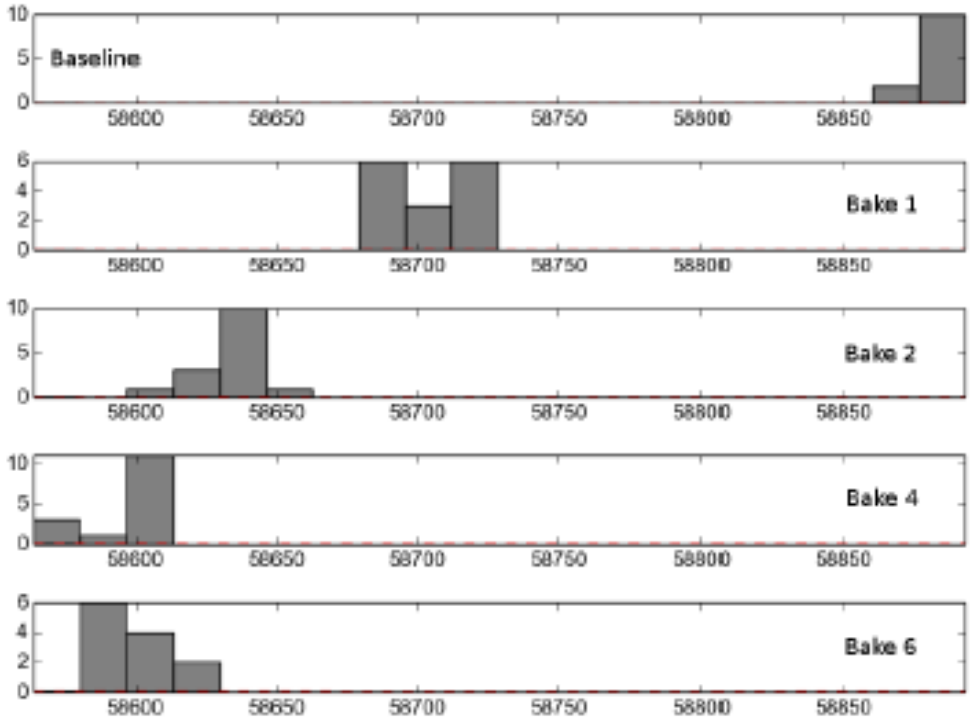

# What can we do with this information?

- **Method for discriminating between FPGA lots.**
- **Used in determining lot integrity.**



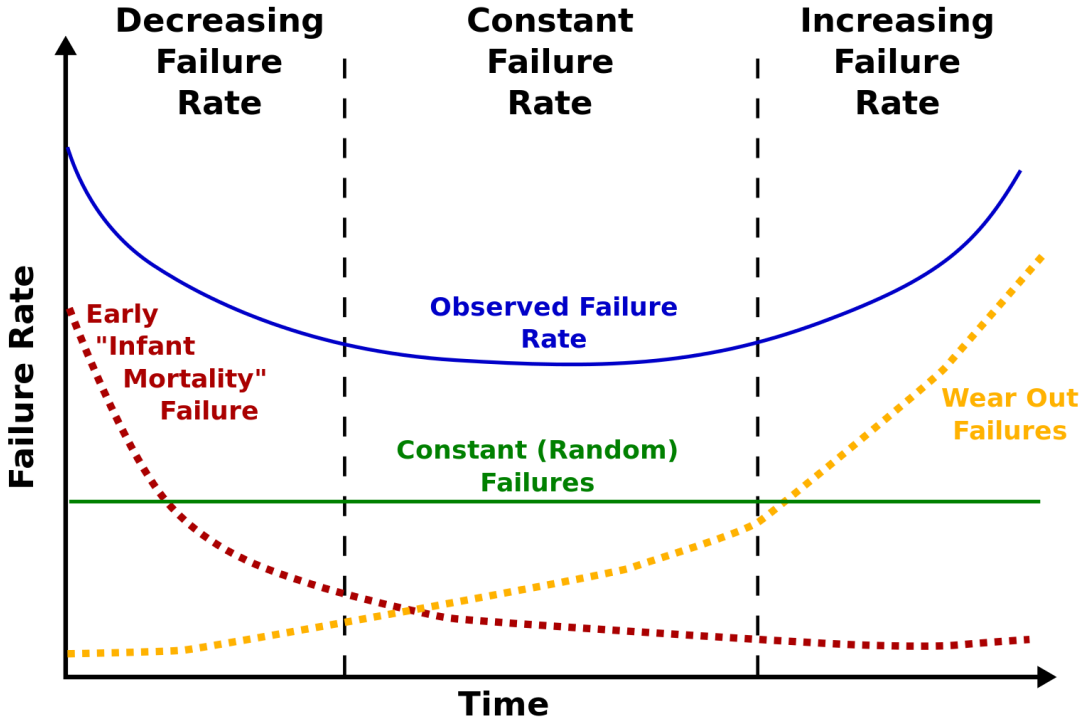
# What can we do with this information?

- **Method for discriminating between baked FPGA chips.**
- **Used for detecting tampered chips with adequate baselines.**



# What are we looking for?

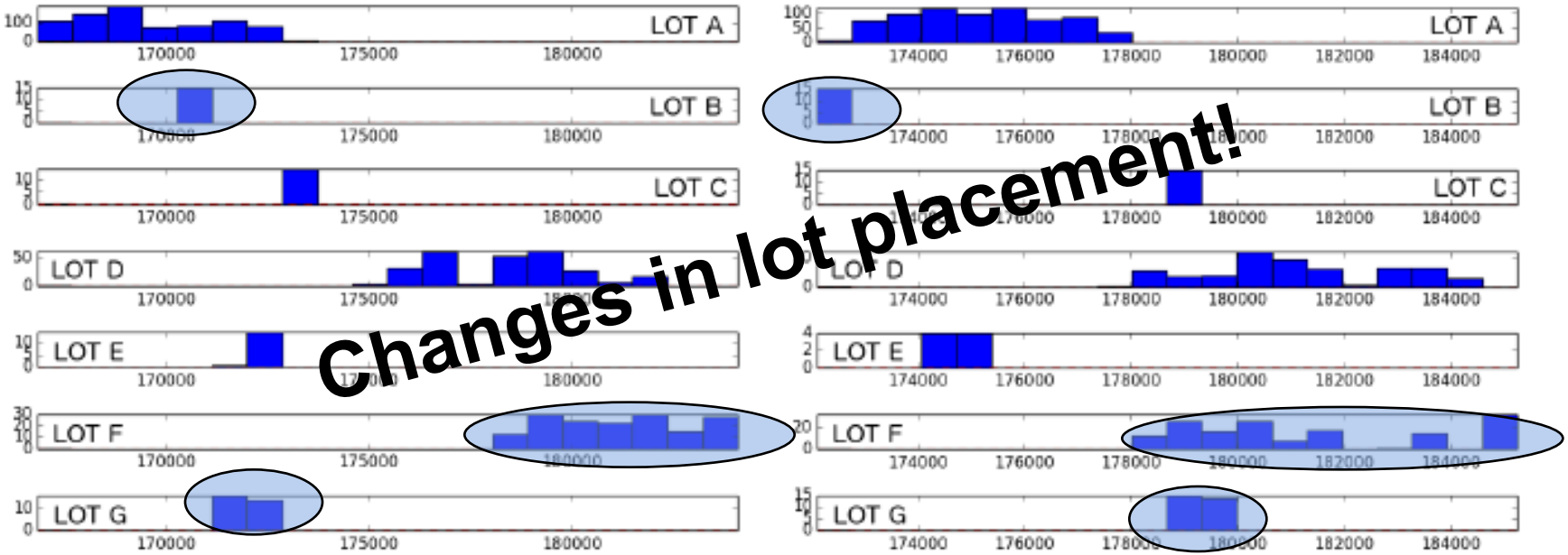
- All chips have a initial burn in procedure.
- If the “Infant Mortality Failure” and Wear Out Failure curves are modified, mission objectives may be compromised. [10]




[10] G. Klutke, P. Kiessler, and M. Wortman, “A critical look at the bathtub curve," IEEE Transactions on Reliability, vol. 52, no. 1, pp. 125-129, Mar 2003.

# Results–Supply Chain Integrity Measurer for FPGAs

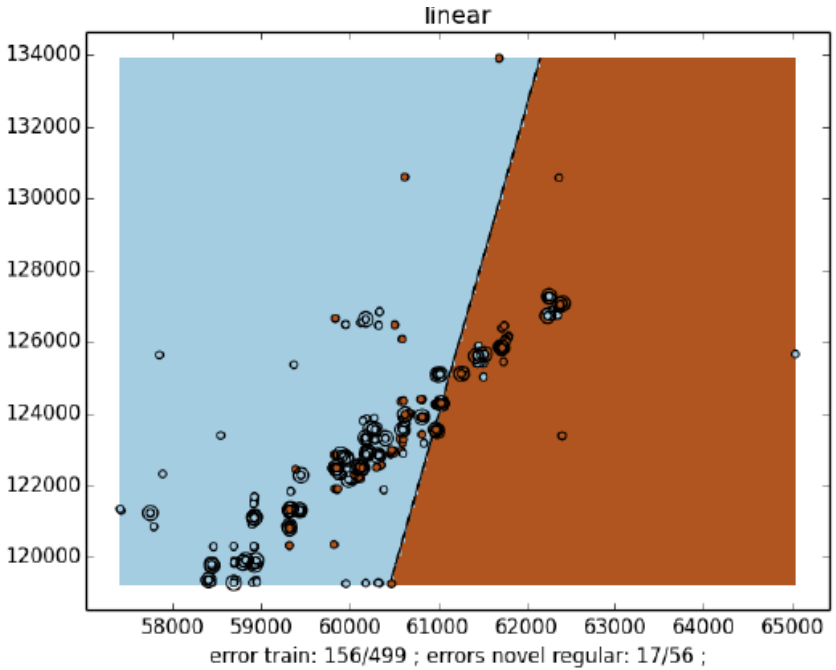
- **Slight differences can be identified between the lots for two different ring oscillators.**

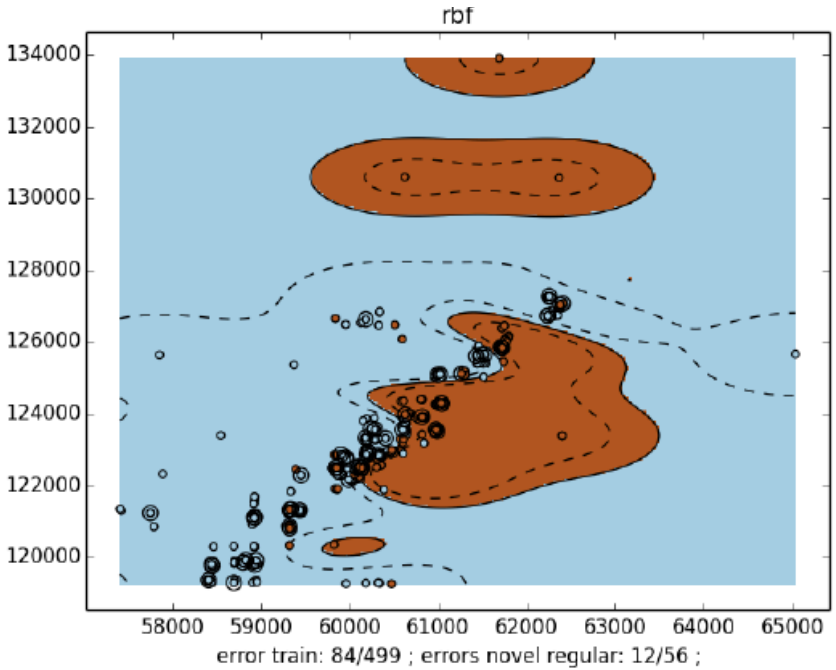



Note: y-axis is frequency in Hertz, y-axis is number of elements in histogram bin.

# Results–Supply Chain Integrity Measurer for FPGAs

- **This data can then be utilized in a Support Vector Machine (SVM) to perform classification of results.**




Note: Both x and y axis are frequency in Hertz.

# Results–Supply Chain Integrity Measurer for FPGAs

- **This can be further expanded to utilize all 8 dimensions of measurements.**
- **Single digit error rates.**

Training

| | Linear | RBF .000005 | RBF .000001 | RBF .0000005 | RBF .0000001 |
|---|---|---|---|---|---|
| .3 | 62/2760 | 0/2760 | 0/2760 | 0/2760 | 0/2760 |
| .5 | 76/4184 | 0/4184 | 0/4184 | 0/4184 | 0/4184 |
| .7 | 128/6120 | 0/6120 | 0/6120 | 0/6120 | 0/6120 |

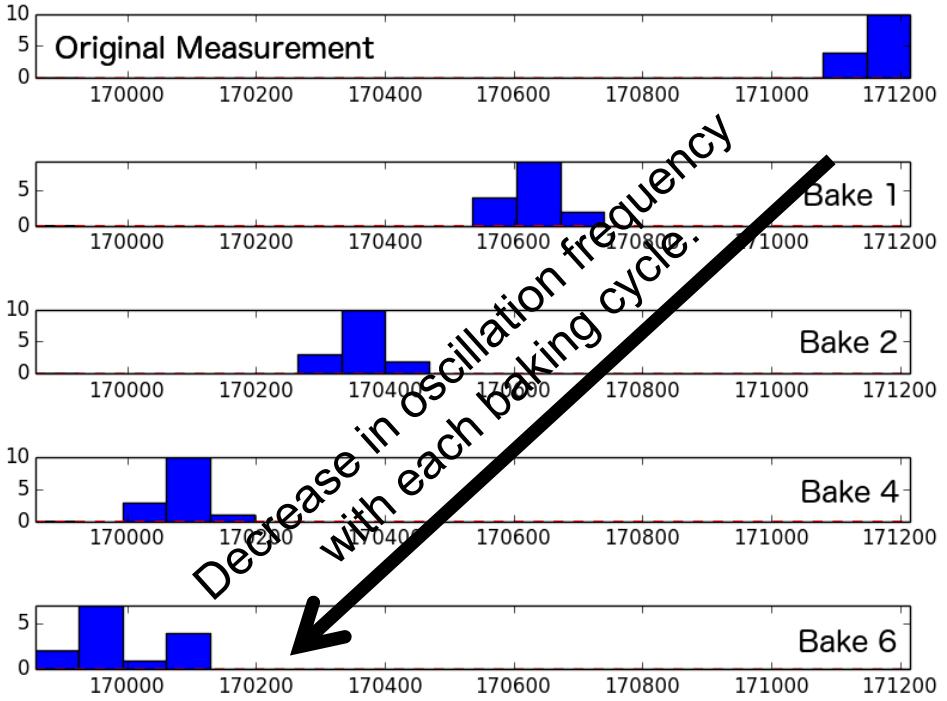
Novel Data

| | Linear | RBF .000005 | RBF .000001 | RBF .0000005 | RBF .0000001 |
|---|---|---|---|---|---|
| .3 | 128/6120 | 227/6120 | 100/6120 | 89/6120 | 84/6120 |
| .5 | 70/4184 | 115/4184 | 54/4184 | 47/4184 | 43/4184 |
| .7 | 45/2760 | 52/2760 | 17/2760 | 18/2760 | 11/2760 |

Note: x-axis is Gamma Values for RBF, y-axis is percentage of training data.

# Results–Supply Chain Integrity Measurer for FPGAs

- This graph shows the gradual decrease in frequency of a part.
- Each part is exposed to multiple baking processes.
  - This simulates the removal from a PCB board in addition to the burn-in process.




Note: y-axis is frequency in Hertz, y-axis is number of elements in histogram bin.

# Results–Supply Chain Integrity Measurer for FPGAs

- **Error rates are higher than the lot identifiers, but are still around 10% for RBF kernels.**

Training Data

| | Linear | RBF .00005 | RBF .00001 | RBF .000005 |
|---|---|---|---|---|
| .3 | 390/1080 | 1/1080 | 1/1080 | 1/1080 |
| .5 | N/A | 0/1800 | 3/1800 | 6/1800 |
| .7 | N/A | 0/2520 | 2/2520 | 8/2520 |
| .9 | N/A | 0/3240 | 3/3240 | 10/3240 |

Novel Data

| | Linear | RBF .00005 | RBF .00001 | RBF .000005 |
|---|---|---|---|---|
| .3 | 1098/2520 | 454/2520 | 287/2520 | 235/2520 |
| .5 | N/A | 242/1800 | 165/1800 | 113/1800 |
| .7 | N/A | 122/1080 | 92/1080 | 77/1080 |
| .9 | N/A | 51/360 | 39/360 | 32/360 |

Note: x-axis is Gamma Values for RBF, y-axis is percentage of training data.

# Analysis—Supply Chain Integrity Measurer for FPGAs

- **How does this fit into existing research?**

| IDs | Reliability | Uniqueness | Unclonable | Manufacturability | Cost effectiveness | Ease-of-Use |
|---|---|---|---|---|---|---|
| QR codes (Physical Artifact) | Not verified | Medium | Medium | Not verified | Not verified | High |
| DNA markings | Low | Low | Low | Low | Low | Medium |
| Nanorods (Physical Artifact) | Not verified | High | High | Not verified | Not verified | Medium |
| Physically Uncloneable Functions | Not verified | High | High | Not verified | Not verified | Medium |
| Scanning Electron Microscope | High | N/A | N/A | N/A | Low | High |
| Chemical Analysis | Medium Low | Low | Low | High | Low | Low |
| Foundry Identification[36] | Medium Low | Low | Low | N/A | Medium | Medium High |
| Recycled FPGA Detection[35] | Medium Low | Medium Low | Medium | N/A | Medium | Medium High |
| Modified RO: Lot-ID | Medium Low | Medium Low | Medium | N/A | Medium | Medium High |
| Modified RO: Life cycle | Medium Low | Medium Low | Medium | N/A | Medium | Medium High |

# Analysis—Supply Chain Integrity Measurer for FPGAs

- **How does this fit into existing techniques?**

| Avoidance Technique | Reliability | Destruct-iveness | Implementation Difficulty | Detection Difficulty | Implementation Cost | Identification Mechanism |
|---|---|---|---|---|---|---|
| Physically Unclonable Functions | Medium | None | Medium | Low | High | Individual die |
| Physically Identifiable Artifact | Low | None | Low | Low | Low | Individual die |
| Scanning Electron Microscope | High | Yes | None | High | None | Difference between two dies |
| Chemical Analysis | Medium Low | Yes | Medium | High | Medium | Difference between two dies |
| Foundry Identification[36] | Medium Low | None | Low | Medium | Medium | Manufacturing foundry |
| Recycled FPGA Detection[35] | Medium Low | None | Low | Medium | Medium | Golden model comparison |
| Modified RO: Lot-ID | Medium Low | None | Low | Medium | Medium | Manufacturin lot |
| Modified RO: Life cycle | Medium Low | None | Low | Medium | Medium | Individual die re-flow |

# *Future Work–Supply Chain Integrity Measurer for FPGAs*

- **Additional vectors of data need to be integrated into the SVM for better analysis.**
  - **More manufacturing lots.**
  - **Advise from vendors on manufacturing processes.**
- **Additional test cases should be evaluated to further fine-tune the ring oscillators.**
  - **Develop process to further identify attribute points.**
  - **Further investigate placement properties.**

# *Conclusions–Supply Chain Integrity Measurer for FPGAs*

- **New technique to actively measure the "health status" of FPGAs.**
  - **Lot/foundry discrimination.**
  - **FPGA aging/baking discrimination.**
- **This status can be used in conjunction with other techniques to improve active measurements of FPGAs to assist with supply chain decisions.**
  - **Assist in obtaining/validating older FPGAs.**

# Acknowledgements


- Thanks to Dr. Peter Athanas, Dr. Jonathan Black, Dr. Charles Clancy, Dr. Robert McGwier, Dr. Neil Steiner for advise on this project and serving on my PhD committee!
- Thanks to Dr. Patrick Schaumont, for advise on the PUFs and ensuring proper Ring Oscillator generation to optimize artifact collection.


# Questions?


JOHNS HOPKINS
APPLIED PHYSICS LABORATORY