REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
14-12-2015	Final Report	12-Sep-2012 - 11-Sep-2013

4. TITLE AND SUBTITLE
Final Report: Workshop on Counterfeit Electronics

5a. CONTRACT NUMBER
W911NF-12-1-0524

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
611102

6. AUTHORS
Mark Tehranipoor

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
University of Connecticut - Storrs
Sponsored Program Services
438 Whitney Road Ext., Unit 1133
Storrs, CT 06269 -1133

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS (ES)
U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSOR/MONITOR'S ACRONYM(S)
ARO

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
63028-CS-CF.1

12. DISTRIBUTION AVAILIBILITY STATEMENT
Approved for Public Release; Distribution Unlimited

13. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT
This workshop was held 2013 at the University of Connecticut. The PI, Prof. Tehranipoor, organized the workshop and invited key researchers and practitioners from academia, research labs, industry and government who are currently working on the above issues. This special workshop was a two day event; the first day started at 8:30am and ended at 5:30pm. The workshop resumed on the second day starting from 8:30am until 5pm. About 15 invited talks were scheduled in the workshop. In addition, a poster session was also organized by students. The workshop participation was only through invitation. However, the PIs graduate students and members of ECE and CSE

15. SUBJECT TERMS
Counterfeit Electronics

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Mohammad Tehranipoor
UU	UU	UU	UU		19b. TELEPHONE NUMBER: 860-486-3471

Report Title

Final Report: Workshop on Counterfeit Electronics

ABSTRACT

This workshop was held 2013 at the University of Connecticut. The PI, Prof. Tehranipoor, organized the workshop and invited key researchers and practitioners from academia, research labs, industry and government who are currently working on the above issues. This special workshop was a two day event; the first day started at 8:30am and ended at 5:30pm. The workshop resumed on the second day starting from 8:30am until 5pm. About 15 invited talks were scheduled in the workshop. In addition, a poster session was also organized by students. The workshop participation was only through invitation. However, the PIs graduate students and members of ECE and CSE departments at UConn attended the workshop as well.

This workshop was aimed at providing a deeper understanding of the counterfeiting issues, discussing foundation of the problem, its impact on critical and non-critical applications, detection techniques, prevention techniques, development of new policies, emerging threats, etc. Currently, many researchers and practitioners in academia, industry, and government are investigating various aspects of the problem such as IC authentication, development of low-cost techniques for detecting counterfeit parts, risk analysis, untrusted foundry, etc. This workshop provided a forum to discuss the above challenging issues, current solutions in addition to help providing a detailed roadmap for researchers and Army Research Office (ARO), and futures trends.

Enter List of papers submitted or published that acknowledge ARO support from the start of the project to the date of this printing. List the papers, including journal references, in the following categories:

(a) Papers published in peer-reviewed journals (N/A for none)

Received Paper

TOTAL:

Number of Papers published in peer-reviewed journals:

(b) Papers published in non-peer-reviewed journals (N/A for none)

Received Paper

TOTAL:

Number of Papers published in non peer-reviewed journals:

(c) Presentations

Number of Presentations: 0.00

Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

Received Paper

TOTAL:

Number of Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

Peer-Reviewed Conference Proceeding publications (other than abstracts):

Received Paper

TOTAL:

Number of Peer-Reviewed Conference Proceeding publications (other than abstracts):

(d) Manuscripts

Received Paper

TOTAL:

Number of Manuscripts:

Books

Received Book

TOTAL:

Received	Book Chapter

TOTAL:

Patents Submitted

Patents Awarded

Awards

Graduate Students

NAME	PERCENT_SUPPORTED

FTE Equivalent:
Total Number:

Names of Post Doctorates

NAME	PERCENT_SUPPORTED

FTE Equivalent:
Total Number:

Names of Faculty Supported

NAME	PERCENT_SUPPORTED

FTE Equivalent:
Total Number:

Names of Under Graduate students supported

NAME	PERCENT_SUPPORTED

FTE Equivalent:
Total Number:

Student Metrics

This section only applies to graduating undergraduates supported by this agreement in this reporting period

The number of undergraduates funded by this agreement who graduated during this period: 0.00

The number of undergraduates funded by this agreement who graduated during this period with a degree in science, mathematics, engineering, or technology fields:..... 0.00

The number of undergraduates funded by your agreement who graduated during this period and will continue to pursue a graduate or Ph.D. degree in science, mathematics, engineering, or technology fields:..... 0.00

Number of graduating undergraduates who achieved a 3.5 GPA to 4.0 (4.0 max scale):..... 0.00

Number of graduating undergraduates funded by a DoD funded Center of Excellence grant for Education, Research and Engineering:..... 0.00

The number of undergraduates funded by your agreement who graduated during this period and intend to work for the Department of Defense 0.00

The number of undergraduates funded by your agreement who graduated during this period and will receive scholarships or fellowships for further studies in science, mathematics, engineering or technology fields: 0.00

Names of Personnel receiving masters degrees

NAME

Total Number:

Names of personnel receiving PHDs

NAME

Total Number:

Names of other research staff

NAME	PERCENT_SUPPORTED

FTE Equivalent:

Total Number:

Sub Contractors (DD882)

Inventions (DD882)

Scientific Progress

Technology Transfer

What were the current state of knowledge in this domain?

- Cost of counterfeiting and piracy for G20 nations estimated at $450-$650B in 2008 and growing to $1.2-1.7T in 2015.
- Standards
  - SAE G19 developed AS5553 and AS6171 (Test Methods Standards), AS6081 (Distributors), and AIR6273 (Terms and Definitions) are in progress.
  - IDEA-STD-1010 (Developed in 2006) and CCAP-101
- Counterfeit parts often pass through numerous channels and difficult to trace back to counterfeiting sources
- Not all types of counterfeit ICs are targeted
  - Detection of Cloned and Tampered ICs are fairly impossible. Most of the presenters talks only recycled/remarked ICs.
- The Problem of “Good” Counterfeits
  - If Test and Inspection is basically Quality, we have a problem

ARO Sponsored Workshop on

Counterfeit Electronics

Mark Tehranipoor

What were the major concerns raised by the speakers?

- Counterfeiting is an emerging and evolving problem and billions of counterfeit ICs circulating in the supply chain.
- Need for continuously monitor of counterfeiters activity.
- Major challenges in hardware assurance, reliability and security.
- Challenges for detection of obsolete/legacy and active components.
- Counterfeits are the #1 threat to electronics reliability!
  - ESD Damage (CMOS gate oxide & Bipolar/BiCMOS capacitors)
  - Popcorning due to mishandling of Moisture-sensitive parts.
  - Chemicals used in Recycling might damage ICs.
  - Violate RoHS requirements.
  - Classic reliability models (such as MIL-HDBK-217 MTBF calculations) are completely meaningless if even one component in a system is counterfeit!
- There were inadequate counterfeit inspection procedures in place at the time of purchase – Concerns about independent distributors (Not registered to ERAI)
- Supplier Approval Weaknesses (Supplier Types: authorized, preferred, acceptable, probationary, and prohibited)

What were the major concerns raised by the speakers? – Cont.

- Training Weaknesses (affected organizations and new hires)
- Newer Counterfeit Techniques Are Far More Sophisticated Than These Conventional Techniques Obsolete
  - Excellent black topping and marking quality/ logs, date and lot codes are perfect/ original dies inside the package
  - Conventional Visual Techniques Not Adequate for Newer Threats
- Latency Problem Has Not Been Addressed
  - Latency and Reliability problems
  - Damage during the die recovery process
  - Bond pad degradation
  - Possible heating issues due to package integrity
  - Potentially high rate of field failures
- Counterfeiters act as “competitors” to legitimate companies.
  - They use our technology to improve their products and sell at a reasonable price to avoid suspicion.
  - They find distribution chains to use or infiltrate and figure out our weaknesses faster than we figure out theirs.
  - Counterfeiters are marketing their products competitively

What were the plans suggested for year 1-5?

- Develop and implement anti-counterfeiting measures
  - DFCA - Design for Counterfeit Avoidance.
- Easy detection of counterfeit parts in any stages of electronic component supply chain.
- Develop test metrics to evaluate the detection methods
- Implementation of automation for detection
  - Data based decision.
- Develop low cost, fast and hand-held (mobile) detection methods.
  - However, Costly Electrical Testing is Inevitable to Detect Latest Counterfeit Techniques
  - Costly Proposition But Cost Can Be Minimized By
    - Use of Smart Test Plan – Don't Need to Test What is not Boeing Used in Application
    - Use Emulators, Simulators, Reference Boards Instead of Developing All New Functional Vectors
  - Functional at-speed
    - Application speed not max spec
    - Test frequency is a major tester cost driver
  - Comprehensive Functional Testing
    - Test all device functionality
    - Fault grading is not possible since only the manufacturer has device modeling capability
- Development of efficient test methods for hardware Trojan detection.

What were the plans suggested for year 1-5? – Cont.

- Solutions to maintain the supply-chain of obsolete parts
- Better traceability & documentation for components in the supply chain.
- Purchase components exclusively from OCMs and their authorized distributors (rather than blindly off the web)
- Technical Investigation and Reporting Requirements
- DNA Marking/ Unique Embedded or OTP Codes on The Device
- Proper Recycling of e-Waste
- Enhanced penalties for breaking anti-counterfeiting laws.

Plans suggested for year 5-10?

- Quantitative and Transparent Risk Assessment and Risk-Based Decision Analysis and Management
- Systems-Based Approach to Risk Management
- Quantitative metrics for counterfeit detection
- Standard design principles for counterfeit avoidance: this should be adaptive and flexible
- Incorporating with social science to build risk decision model for supply chain
- Removing the need for obsolete parts, and developing new system qualifications to change to the new parts
- Developing infrastructure to validate authenticity at all levels of the value chain
- Use multiple levels to enable the right combination of authentication
- Designing parts with the features embedded at the smallest node sizes which can only be replicated in comparable fabs.
- Expanding trusted foundries for critical applications.

Research opportunities for Academia?

- Design for Counterfeit Avoidance
- Designing test methods that can determine if a device was previously used and for what duration
- Unique Embedded or OTP Codes on The Device
- Adaptive decision making and risk assessment
- Exploiting the biometrics in the silicon devices to detecting counterfeit parts
- Designing multiple levels to enable right combination of authentication
- Quantitative metrics for counterfeit detection
- Device signatures for counterfeit avoidance

Summary of panel 1

- Testing for counterfeit detection should be consistent from lab to lab to avoid false negative and false positive. Standardization is important.
- Testing labs should improve the quality of testing and testing techniques
- Counterfeits are evolving, so we need to monitor and improve our techniques too
- Success of the techniques are heavily dependent on the money and time consumed for the part
- Concern about the labs, Which lab can we trust ?
  - Proficiency test that can verify that a lab or engineer is qualified for the task.

Summary of panel 1 – Cont.

- Evaluating if a part is counterfeit or not is so subjective because of the nature of counterfeiting problem
- Proficiency programs and certification programs should be operator level, each operator should be certified to perform specific test and certified labs should consist of those operators.

Summary of panel 2

- Adaptive Decision Support tools: fusing Risk Analysis, Decision Analysis, and Cognitive Modeling
  - Risk Assessment to Risk-Based Decision Analysis and Management
- For Counterfeit Detection
  - Physical Unclonable Function (PUF)
  - DNA Marking, for tagging of chips
  - Functional Evaluation
  - Silicon Biometrics
- Concerns about academia
  - Highly trained students can potentially add counterfeiters activity.
- Counterfeiting is basically a supply chain problem
- Combined methods provide multiple layers of identification
  - Encrypted 2D bar code using taggants, micromarking and bar coding, taggants with 2 programmable properties, etc.
- Introduction to a novel authentication platform
- Functional Clones are the final frontier of the counterfeiter
- Current Status of the Various Industry Standards for Mitigating Counterfeits
- Challenges Ahead for Both Obsolete and Current Technology Products
- Recommendations for Counterfeit Parts Avoidance

Report on the posters (you can the title of all posters)

- Mohammad Tehranipoor, “SST: Secure Split-Test for Preventing IC Piracy and Easy Detection”, CHASE, UConn
- Hassan Salmani and Mohammad Tehranipoor, “Trust Benchmarks and Design Vulnerability Analysis”, CHASE, UConn
- Xiaoxiao Wang and Mohammad Tehranipoor, “Low-Cost On-Chip Structures for Measuring NBTI Effects, Variations, Path Delay, and Noise”, CHASE, UConn
- Xuehui Zhang, Nicholas Tuzzio, and Mohammad Tehranipoor, “Identification of Recovered ICs Using Fingerprints from a Light-Weight On-Chip Sensor”, CHASE, UConn
- Xuehui Zhang, Nicholas Tuzzio, and Mohammad Tehranipoor, “RON: On-Chip Ring Oscillator Network for Hardware Trojan Detection”, CHASE, UConn
- Jifeng Chen, Shuo Wang, and Mohammad Tehranipoor, “Timing Analysis and Gate Sizing Considering Aging Effects”, CHASE, UConn
- Kan Xiao, Xuehui Zhang and Mohammad Tehranipoor, “Hardware Trojan Detection Using Clock Sweeping Technique”, CHASE, UConn
- Kan Xiao and Mohammad Tehranipoor, “Prevention of Trojan Insertion Using Built-In Self-Authentication”, CHASE, UConn

Report on the posters (you can the title of all posters)

- Ujjwal Guin and Mohammad Tehranipoor, “Counterfeit Detection and Technology Assessment”, CHASE, UConn
- Md. Tauhidur Rahman and Mohammad Tehranipoor, “Aging Resilient Physical Unclonable Functions”, CHASE, Uconn
- Kun Yang, Xuehui Zhang, Tauhidur Rahman, and Mohammad Tehranipoor, “Contactless Counterfeit IC Detection”, CHASE, UConn
- Shane Kelly, Xuehui Zhang, Andrew Ferraiuolo and Mohammad Tehranipoor, “Experimental Analysis of a Ring Oscillator Network for Hardware Trojan Detection in a 90nm ASIC”, CHASE, UConn
- Joseph LaRosa, Nathan Murphy, Shane Kelly and Mohammad Tehranipoor, “Counterfeit Detection and Evaluation Board”, CHASE, UConn
- Zhijie Shi, Chujiao Ma, Fan Zhang, “Efficient and Secure Computing”, UConn
- H. Lin, X. Guan, Y. Fei, and Z. Shi, “Architectural Enhancement for Program Code Integrity Monitoring in Application-specific Instruction Set Processors”, UConn

Conclusions

- The threat of counterfeit parts to hardware assurance, security and reliability is increasing significantly.
- The current status of counterfeit detection, prevention and its challenges ahead are discussed in detail.
- Various inspection, test, and evaluation methods and tools for counterfeit detection are presented.
- Advanced techniques for combating counterfeit are introduced, including three dimensional computational imaging using quantum optics, physical unclonable function (PUF), DNA marking , silicon biometrics etc.
- A variety of standards, specifications, and protocols about counterfeit detection are discussed.
- The prevention of counterfeit parts needs collaboration among industry , academia and government.
- Various projects related to Counterfeit Detection, Hardware Security and Reliability are presented by CHASE Students during poster sessions.