Jim Plusquellic

ECE Department, University of New Mexico
MSC01 1100, 1 University of New Mexico
Albuquerque, NM 87131-0001
Office: 505-277-0785, Cell: 240-475-1882, FAX: 505-277-1349
jimp@ece.unm.edu, http://ece-research.unm.edu/jimp/

Education

Ph.D.	1997	University of Pittsburgh, Computer Science
M.S.	1995	University of Pittsburgh, Computer Science
B.S.	1983	Indiana University of Pennsylvania, Biology

Work Experience

2018-present	CEO and President, Integrated Circuit Secure Authentication, Fingerprinting and Encryption in Trusted Systems (IC-Safety), LLC
2016-present	CTO, Enthentica Inc.
2014-present	Full Professor, ECE Dept., Univ. of New Mexico
2014-present	CEO and President, Trusted and Secure Systems (TruSecSys), LLC
2014-2015	Sabbatical at Sandia National Laboratories
2008-2014	Associate Professor, ECE Dept., Univ. of New Mexico
2011-2018	Magic Dragon Technologies, LLC
2003-2008	Associate Professor, CSEE Dept., Univ. of Maryland, Baltimore County
2006	NASA Faculty Fellowship Program, NASA, Goddard (June-Aug.)
2003-2004	Sabbatical at IBM Austin Research Laboratory (Sept.-May) and National Institute of Standards and Technology (June-Aug.)
1997-2003	Assistant Professor, Univ. of Maryland, Baltimore County

Honors and Awards

- Selected tutorial at HOST, "Side Channel Attacks and Countermeasures", 2019.
- Appointed Editor-in-Chief, *Hardware Security Section of Cryptography, MDPI*, 2018.
- Inducted into the IEEE International Symposium on Hardware-Oriented Security and Trust **Hall-of-Fame**, May, 2018.
- Appointed Editorial Board, *Cryptography, MDPI*, 2017

- **Outstanding Contribution Awards**, IEEE Computer Society, "In Recognition as Co-Founder of and providing Outstanding Contributions to the IEEE International Symposium on Hardware-Oriented Security and Trust (HOST) for the Past Ten Years 2008-2017", 2017
- Selected IoT PUF-based Authentication tutorial at HOST, "*Hardware Security and Trust Challenges in Emerging IoT Systems and Applications*", 2017 & 2018
- Recipient of "*Albuquerque Lab-to-business accelerator"* award, Jan. 2016
- *2014 Innovation Award*, Science and Technology Center at the Univ. of New Mexico, 2014
- *Invited Participant*, *"Design for Security Working Meeting"*, Sponsored by US Army Research Office and USC/ISI, July, 2014
- *Invited Participant*, "Secure, Trustworthy, Assured and Resilient Semiconductors and Systems (STARSS) Workshop", Sponsored by SRC-T3S, May. 21-22, 2014
- *Featured Entrepreneur,* Science and Technology Center at the Univ. of New Mexico, Calendar for 2014
- *Featured Entrepreneur*, School of Engineering, Univ. of New Mexico (*soe.unm.edu/publications/2013/puf-goes-the-hacker.html*)
- *Invited Talk*, "An Embedded Test Structure for Improving Yield Learning, Profiling New Product Introductions and for Implementing Hardware Security Primitives", Intel FSM College of Engineering, Technical Seminar Series, March 2013
- **Golden Core Member**, IEEE Computer Society, Jan. 2013
- *Invited Participant*, "Convergence of Software Assurance Methodologies and Trustworthy Semiconductor Design and Manufacture", Sponsored by NSF, SRC and CCC, Jan. 15-16, 2013
- **Outstanding Contribution Award**, IEEE Computer Society, "In Recognition as Co-Founder of and providing Outstanding Contributions to the IEEE International Symposium on Hardware-Oriented Security and Trust (HOST) for the Past Four Years 2008-2012", June 3, 2012
- Awarded *Best IP Session for VTS 2011*, VLSI Test Symposium (VTS), Jan. 2012
- International Test Conference, *10 Years of Continuous Service Award*, Oct. 2011
- Appointed *TTTC Technical Activity Chair*: Hardware Security and Trust, Sept. 2011
- Appointed *Associate Editor*, Transactions on Computers, Feb. 2011
- Structural Tester Donation (Ocelot ZFP Tester) from Verigy, June 2010
- ***General Chair***, Hardware-Oriented Security and Trust, June 2010
- **Co-founder** of IEEE International Workshop on Hardware-Oriented Security and Trust (HOST), June, 2008 (with Mohammad Tehranipoor)
- *General Chair*, Defect-Based Testing Workshop, Oct. 2006

- International Test Conference, *5 Years of Continuous Service Award*, Oct. 2006
- VLSI Test Symposium *Best Paper Award*, May 2005
- ACM *Distinguished Service Award*, "For Exemplary Service to ACM/SIGDA and the Design Automation Conference as Director of the University Booth Program", June 2003
- *IBM Visiting Scholar*, Austin Center for Advanced Studies, IBM Austin Research Laboratory, June-July 2001
- Awarded 2001 and 2002 *Austin CAS Fellow Award*
- Awarded the *Pennsylvania Space Grant Consortium Fellowship*, Aug. 1995

Research Support

2020-present	Sandia National Laboratories, "FPGA Dynamic Partial Reconfiguration Approach to Modeling Fault Injection Attacks on FPGAs and Microprocessors", $90K, P.I.
2019-present	Sandia National Laboratories, "FPGA Dynamic Partial Reconfiguration Approach to Modeling Fault Injection Attacks on FPGAs and Microprocessors", $80K, P.I.
2018-present	NSF SaTC: CORE: Small: Collaborative: Techniques for Enhancing the Security and Trust of FPGAs-Based Systems, 500K total, P.I., $200K to UNM, $200K to UMBC and $100K to UNCC.
2018-present	Company sponsored award titled "Investigation of Security Film Properties", $80K, P.I.
2016-present	Corporate and investor funding for commercialization activities
2011-2016	SHF: Small: Measurement and Analysis of Regional Process Variations using Existing and Minimally Invasive On-Chip Embedded Resources, $300,000, P.I.
2010-2014	ATE Project: Developing the Digital Technologist for the New Millennium, NSF, $700,000, Co-P.I.
2010-2015	TC: Small: Collaborative Research: Exploration and Validation of Hardware Primitives for Security and Trust, NSF, $500,000, P.I.
2007-2011	CT-ISG: Detection and Isolation of Malicious Inclusions in Secure Hardware (DIMINISH), NSF, $150,000, P.I.
2007-2008	Controller Design for Time-to-Digital Conversion Time-of-Flight Chip, NASA, $13,000, P.I.
2007-ongoing	Embedded Test Structures for Variation Analysis, Access to IBM's 65 nm and 90 nm PDK, future funding opportunities, IBM ARL, P.I.
2006-2007	RF-ADC Chip Test Project, $30,000, NASA, Co-P.I.

2005-2006	RF-ADC Chip Design Project, $85,000, NASA, Co-P.I.
2004-2006	Defect Based Test for Detection and Localization, $20,000, IBM Faculty Partnership Award, P.I.
2003-2004	Power Supply Signal Analysis for Defect Detection, Fault Localization and Diagnosis, $40,000, IBM Faculty Partnership Award, P.I.
2001-2004	Production-Oriented V_{DDT} and I_{DDQ} Device Testing Methods Based on Multiple Power Supply Pad Measurements, $318,000, NSF, P.I.
2002-2003	Novel VLSI Testing and Diagnostics Methods for Silicon Technology, $40,000, IBM Faculty Partnership Award, P.I.
2002-2003	Hardware Verification of Novel Power Supply Defect Detection and Diagnosis (research chip fabrication grant), ~$10,000, NSF, P.I.
2001-2002	Multiple Power Supply Pad V_{DDT} Testing for Delay Faults, $25,000, IBM Faculty Partnership Award, P.I.
2001-2002	Dynamic Transport Selection for Mobile Computing, $50,000, Aether grant, Co-P.I.
2000-2001	Fitting Rovibronic Spectra with Genetic Algorithms, $10,000, NIST grant, P.I.
2000-2001	Multiple Power Supply Pad V_{DDT} Testing for Delay Faults, $25,000, IBM Faculty Partnership Award, P.I.
2000-2001	Simulator to Evaluate/Prototype Local Area and Personal Area Wireless Network Protocols and Products, $80,000, Aether grant, Co-P.I.
1999-2000	Power Supply Transient Signal Analysis for Defect Detection using the FISHNET ASIC, $74,194, DOD, P.I.

Sabbaticals and Off-Site Work Experiences

Sabbatical at Sandia National Laboratories (Sept. 2014-Aug. 2015)

NASA Faculty Fellowship Program, NASA, Goddard (June-Aug. 2006)

IBM Austin Research Laboratory (Sept. 2003-May 2004)

National Institute of Standards and Technology (June-Aug. 2004)

Equipment and Chip Fabrication Donations

2011	**~$100K from Remington Test for 2 Micromanipulator 8860 Probe Stations**
2010	**~$400K from Verigy for Ocelot ZFP Tester**

2010	~$30K from MOSIS, MEP Research support program to build a chip in IBM's 10LPe (90 nm Low Power CMOS), Project Title: "Exploration of Validation of Hardware Primitives for Security and Trust"
2008	~$50K from AFRL, SemiProbe IC packaging instrument and PCB fabrication equipment including pick-and-place/re-flow oven.
2003-2004	~$80K from Tektronics for teaching laboratories
2003-2004	~$20K from Xilinx for teaching laboratories
2002-2003	$13,360, Intel equipment grant
2001-2002	$2,701, Xilinx FPGA/software grant
1999-2000	$17,808, Intel equipment grant
1999-2000	$12,500, DRIF award, UMBC
1997-1998	Lockheed Martin Faculty Development, $3,000, UMBC

Students

Current Ph.D. Students

Derek Heeger, ABT

Ian Wilcox , pre-proposal

Don Owen, pre-proposal

Austin Timothy Owens, pre-proposal

Current M.S. Students

Jithin Joseph

Sriram Thotakura

Ryan Lee Fleming

Idris Olansile Somoye

Ph.D. Degrees Awarded

Mitchell Martin, 2020, **chair**, Sandia National Laboratories, "Physical Unclonable Functions Based on Delay Paths and an Interdigital Microstrip Notch Filter"

Xu Zhang, 2017, member

Wenjie Che, 2016, **chair**, New Mexico State University, "Model Building and Security Analysis of PUF-based Authentication"

Dylan Ismari, 2015, **chair**, Micro-RDC, "Detecting Delay Anomalies Introduced by Hardware Trojans Using Chip-Averaging and An On-Chip High Resolution Embedded Test Structure"

Edward Nava, 2015, member

Fareena Saqib, 2014, **chair**, University of North Carolina, Charlotte, "Within-Die Variation Measurement and Analysis Using an Embedded Test Structure REBEL"

Raj Chakraborty (w/ distinction), 2014, **chair**, Intel Corp., Thesis title "Novel Transistor Resistance Variation-based Physical Unclonable Functions with On-Chip Voltage-to-Digital Converter Designed for Use in Cryptographic and Authentication Applications"

Ali Arabi M. Shahi, 2014, member

Pearlson Prashanth Austin Suthanthiraraj, 2013, member

Jing Ju, 2013, **chair**, faculty position at Hunan University of Science and Technology, Thesis title "A Physical Unclonable Function Based on Inter-Metal Layer Resistance Variations and an Evaluation of its Temperature and Voltage Stability"

Jim Aarestad, 2013, **chair**, currently working for COSMIAC, Thesis title "A Hardware-Embedded, Delay-Based PUF Engine Designed for Use in Cryptographic and Authentication Applications"

Matthew Areno, 2013, **chair**, currently working Raytheon, Thesis title "Strengthening Embedded System Security with PUF Enhanced Cryptographic Engines"

Charles Lamech (w/ distinction), 2012, **chair**, joined Intel Corp. Thesis title: "A Truly Embedded Test Structure for Design-for-Manufacturability, Hardware Security and VLSI Testing"

Ryan Helinski (w/ distinction), 2010, **chair**, joined Sandia National Laboratory, Thesis title "A Physical Unclonable Function Derived from the Power Distribution System of an Integrated Circuit"

Mikhail Itskovich, 2009, **chair**, joined Atmel, Thesis title "VLSI Design of an Integrated System for Iddt Testing"

Dhruva Acharyya, 2008, **chair**, joined IBM ARL, now with Advantest Inc., Thesis title "Hardware Results Demonstrating the Effectiveness of Defect Detection and Fault Localization Using Multiple Supply Pad Based IDDT Measurements"

Reza MohammadPourrad, 2008, **chair**, research associate UNM, ST Micro, Thesis title "Detection and Localization of Hardware Trojans through Analysis of Power Ports Transient Signals"

Tom Goff, 2006, member

Abhishek Singh, 2005, **chair**, joined NVidia, Thesis title "An Analytical Framework for Defect Simulation and Estimation of Power-grid Effects in Defect-based Test Methodologies"

Xiao Lin, 2005, member

Chintan Patel, 2004, **chair**, Assistant Prof. UMBC, Thesis title: "Defect Detection and Diagnosis Using Quiescent Signal Analysis"

Eliza Yingzi Du, 2003, member

Naomi Avigdor, 2002, member

William Freeman, 2000, member

MS Degrees Awarded

Ivan Bow, (thesis), 2020, **chair**

Pavlos Athanasios Apostolopoulos, (thesis), 2019, member

Marcos P Torres, (thesis), 2019, member

Nahome Girmahun Bete, (thesis), 2018, **chair**

Jeffrey Denton Calhoun, (thesis), 2018, **chair**

Venkata Varahagiri, (project), 2018, **chair**

Allan Philip, (project), 2018, **chair**

Steven Ruiz, (CO) 2018, **chair**

Casey Alexander Petersen, (thesis), 2018, **chair**

Meghanath Nakka (project), 2017, **chair**

Jacob Nathaniel Healy, 2017, member

Abdelrahman Elshafiey, 2017, member

Venkata Kishore Kajuluri (project), Nov. 2016, **chair**

Athul Balan Edichery Alinkeezhil (project), Nov. 2016, **chair**

James Richard Hemsing (project), Nov. 2016, member

Goutham Pocklassery (thesis), July, 2016, **chair**

Bill Cavanaugh (thesis), June, 2016, **chair**

Akshay Sudhir Vaidya (thesis), Oct. 2015, **chair**

Amanda Bonnie, June, 2015, member

Yuxing Lin, April, 2015, member

Matt Briggs (thesis), Oct. 2014, member

Carlos Montoya (project), Nov. 2013, **chair**

Robert Wayne Sanchez, Nov. 2013, member

Swathi Jagannath (project), July, 2013, member

John Vranes (project), July, 2013, member

Michael Basile (project), June, 2013, **chair**, Thesis title "Creation of Standard Cell Library and Full Synthesis of FPU using IBM 130nm Technology"

Phani Kumar Kandregula (project), April, 2013, member

Joshua Trujillo (project), November, 2012, **chair**

Mike Echert (project), October, 2012, member

Kanamu Pupuhi (project), October, 2012, member

Tony Maokhamphiou (project), July, 2012, **chair**

Thomas LeBoeuf (project), November, 2011, member

Paco Maldonado (project), November, 2011, member

Mirza (project), November, 2011, member

Mitchell Martin (project), April, 2011, **chair**

Michael Thomas (thesis), April 2011, **chair**, Thesis title "Physics-Based Model and Data Analysis for the Estimation of Transverse Flowing Particles"

Jim Aarestad (thesis), April 2011, **chair**, Thesis title "Characterizing Within-Die and Die-To-Die Delay Variation Introduced by Process Variations and SOI History Effect"

Naveen Purushotham (project), November, 2010, member

Shyam Kottaman (project), July, 2010, member

Fareena Saqib (thesis), May, 2010, member

Greg Feucht (thesis), April, 2010, **chair**, Thesis title "Design and Control of a Cellular Architecture-based Adaptive Wiring Manifold"

Andrea Wright (project), April, 2010, member

Soumik Banerjee (project), March, 2010, member

Srikanth ... (Nasir's student), December, 2009, member

Yang Song (project), November, 2009, member

Sev Shelley (thesis), November, 2009, member

Colby Hoffman (thesis), July, 2009, member

Jason R Hamlet (thesis), March, 2009, member

Ryan Helinski, (thesis), July, 2008, **chair**, Thesis title "Measuring Power Distribution System Resistance Variations for Application to Design for Manufacturability and Physical Unclonable Functions"

Shiva Selvarajan, (thesis), June, 2008, **chair**, Thesis title "Building Benchmark Designs For Trojan Experiments"

Joshua Lottich, (thesis), April, 2007, member

Li Deng (project), Jan. 2007, **chair**

Haricharan Kotagiri (thesis), Dec. 2006, member

Mahesh Balakristin (thesis), Sept. 2006, **chair**

Prasath Periyasamy (thesis), Aug. 2006, member

Mohammed ElShoukry (thesis), Aug. 2006, member

Pei Huang (project), Aug. 2006, **chair**

Hok Tang (thesis), Nov. 2005, member

Jitin Tharian (thesis), March 2005, **chair**, Thesis title "On-Chip Digital Signature Generation for Power Supply Transient Signals"

Pushkar Pulastya (thesis), Aug. 2004, **chair**, Thesis title "Reducing Test Application Time for System-on-Chip Testing"

Junping Zhang (project), Dec. 2004, member

Smita Pawar (project), Aug. 2003, **chair**

Shanmugavel Ponnusamy (thesis), Nov. 2002, member

Sanat Kamal Bahl (thesis), Aug. 2002, **chair**, Thesis title "Comparison of Initial Cell Search Algorithms for W-CDMA Systems"

Abhishek Singh (thesis), Aug. 2002, **chair**, Thesis title "Analytical Framework of Transient Signal Analysis and its Evaluation under Real Process and Test Hardware Models"

Chintan Patel (thesis), Aug. 2001, **chair**, Thesis title "Power Supply Transient Signal Integration Circuit"

Ying Ouyang (thesis), Aug. 2000, **chair**, Thesis title "Quiescent Signal Analysis for IC Diagnosis"

Amy Germida (thesis), Jan. 2000, **chair**, Thesis title "8-bit Multiplier Simulation Experiments Investigating the Use of Power Supply Transient Signal Analysis for the Detection of Fabrication Defects in CMOS Integrated Circuits"

Felix K. Watson (thesis), July 1999, member

Zheng Yan (project), Aug. 1999, **chair**

Chuan-Fu Lin (project), May 1999, **chair**

Krishnakamar Sivasankaran (thesis), Sept. 1998, member

Undergraduate Student Research

Charles Helmich, 2018-2019, Charles is working on developing a eCash protocol using PUFs on an Audrino Vidor board

Kevin Barnette, 2017-2019, Kevin is working on building a PCB for hardware security experiments.

Adam Goldstein, Spring and Fall, 2017, Adam designed a CAN bus architecture using Xilinx Zynq 7010 FPGAs, which later became his senior project.

Thomas Bauer, Spring 2012, Tom will be designing a PCB for use in a prototype of an OpAmp based comparator scheme for a Physical Unclonable Function.

Ghadeh Hadi, Summer 2010, Ghadeh is helping with the design of a 65 nm chip using Cadence.

Ghadeh Hadi, Summer 2009, Ghadeh is working with my graduate students to setup our Integrated Circuit Hardware Analysis Laboratory (IC-HAL).

Ryan Helinski, Fall-Spring, 2006-07, Ryan is coding an ATPG algorithm to determine fault coverage for our small delay fault detection strategy.

Kory Schoenfliess, Spring and Summer 2003, TSMC 0.18um standard cell library.

Michael Riggs, Summer and Fall, 2002, Performance and area comparison of several CORDIC algorithms using FPGAs.

Johnathan Hudson, Ryan Robucci, Amir Rowhanirad, Ernesto Staroswiecki. Supervised these recipients of the 2001 Provost's Undergraduate Research Award for a entitled "Home Automation Implemented Using a Low-Cost Reconfigurable Hardware Module", UMBC Review, 2002. (Ryan is now a graduate student at Georgia Tech).

Jonathan Hudson, Summer 1999, Winter 2000, Summer 2000.

Ernesto Staroswiecki, Summer 1999, Summer 2000. (Ernesto spent the summer of 2003 as an intern at IBM's Austin Research Lab and is now a graduate student at Stanford).

Publications

Book Chapters

1. "Hardware Trojan Detection Schemes Using Path Delay and Side-Channel Analysis", Springer Link, 2019.
2. "Detecting Hardware Trojans using Delay Analysis" in book "The Hardware Trojan War: Attacks, Myths, and Defenses", Springer Link, 2017.
3. "*VLSI Test and Hardware Security Background for Hardware Obfuscation*" in book "Hardware Protection through Obfuscation", Springer Link, 2017.
4. "*PUF-Based Authentication*" in book "Fundamentals of IP and SoC Security, Design, Verification, and Debug", Springer Link, 2016.

Journal Publications

1. M. Martin and J. Plusquellic, "NotchPUF: Printed Circuit Board PUF Based on Microstrip Notch Filter", *MDPI*, 2020.
2. I. Bow, N. Bete, F. Saqib, W. Che, C. Patel, R. Robucci, C. Chan and Jim Plusquellic, "Side-channel Power Resistance for Encryption Algorithms using Implementation Diversity", *MDPI*, 2020.
3. J. Calhoun, C. Minwalla, C. Helmich, F. Saqib, W. Che, J. Plusquellic, "Physical Unclonable Function (PUF)-Based e-Cash TransactionProtocol (PUF-Cash)",

MDPI, 2019.

4. J. Plusquellic and M. Areno, "Correlation-Based Robust Authentication (Cobra) using Helper Data Only", Cryptography, *MDPI*, 2018.
5. D. Owen Jr., D. Heeger, C. Chan, W. Che, F. Saqib, M. Areno and J. Plusquellic, "An Autonomous, Self-Authenticating and Self-Contained Secure Boot Process for FPGAs, Cryptography", *MDPI*, 2018.
6. W. Che, F. Saqib and J. Plusquellic, "Novel Offset Techniques for Improving Bitstring Quality of a Hardware-Embedded Delay PUF", *Trans. on VLSI*, 2018.
7. W. Che, V. K. Kajuluri, F. Saqib and J. Plusquellic, "Leveraging Distributions in Physical Unclonable Functions", *Cryptography*, 2017.
8. A. S. Siddiqui, Y. Gui, J. Plusquellic and F. Saqib, "A Secure Communication Framework for ECUs", *Advances in Science, Technology and Engineering Systems Journal*, Special issue on Recent Advances in Engineering Systems, 2017, pp. 1307-1313.
9. W. Che, V. K. Kajuluri, M. Martin, F. Saqib and J. Plusquellic, "Analysis of Entropy in a Hardware-Embedded Delay PUF", *Cryptography*, 2017.
10. W. Che, M. Martin, G. Pocklassery, V. K. Kajuluri, F. Saqib and J. Plusquellic, "A Privacy-Preserving, Mutual PUF-Based Authentication Protocol", *Cryptography*, Vol. 1, Issue 1, 2016.
11. F. Saqib, M. Areno, J. Aarestad and J. Plusquellic, "An ASIC Implementation of a Hardware-Embedded Physical Unclonable Function", *IET Computers & Digital Techniques*, Vol. 8, Issue 6, Nov. 2014, pp. 288-299.
12. F. Saqib, D. Ismari, C. Lamech and J. Plusquellic, "Within-Die Delay Variation Measurement and Analysis Using An Embedded Test Structure", *IEEE Trans. on VLSI*, Vol. PP, Issue 99, May, 2014.
13. F. Saqib, A. Dutta, J. Plusquellic, P. Ortiz, M. S. Pattichis, "Pipelined Decision Tree Classification Accelerator Implementation in FPGA (DT-CAIF)", *IEEE Trans. on Computers*, Volume: PP , Issue: 99, pp. 1, Oct. 2013.
14. J. Aarestad, P. Ortiz, D. Acharyya and J. Plusquellic, "HELP: A Hardware-Embedded Delay-Based PUF", *IEEE Design and Test of Computers*, Vol. 30, Issue: 2, Mar., 2013. pp. 17-25.
15. M. Abramovici, D. Agarwal, S. Bhunia, P. Bradley, M. S. Hsiao, J. Plusquellic and M. Tehranipoor, "Protection against Hardware Trojan Attacks: Towards a Comprehensive Solution", Volume: PP, Issue: 99, *IEEE Design and Test of Computers*, 2013, pp. 6-17.
16. H. Salmani, M. Tehranipoor and J. Plusquellic, "A Novel Technique for Improving Hardware Trojan Detection and Reducing Trojan Activation Time", *IEEE Transactions on VLSI*, Volume: 20, Issue: 1, 2012, pp. 112-125.
17. C. Lamech, R. Rad, M. Tehranipoor and J. Plusquellic, "An Experimental Analysis of Power and Delay Signal-to-Noise Requirements for Detecting Trojans and Methods for Achieving the Required Detection Sensitivities"

IEEE Trans. Information Forensics and Security, Volume: 6, Issue: 3, Part: 2, 2011, pp. 1170-1179.

18. J. Aarestad, D. Acharyya, R. Rad and J. Plusquellic, "Detecting Trojans Though Leakage Current Analysis Using Multiple Supply Pad I_{DDQ}s", *IEEE Transactions on Information Forensics and Security*, Volume: 5, Issue: 4, 2010, pp. 893-904.
19. R. M. Rad, M. Tehranipoor, J. Plusquellic, "A Sensitivity Analysis of Power Signal Methods for Detecting Hardware Trojans under Real Process and Environmental Conditions", *IEEE Transactions in VLSI*, Volume: 18, Issue: 12, 2010, pp. 1735-1744.
20. R. M. Rad, J. Plusquellic, "A Novel Fault Localization Technique Based on Deconvolution and Calibration of Power Pad Transients Signals", *Journal of Electronic Testing, Theory and Applications*, Volume 25, Numbers 2-3, June 2009.
21. R. Helinski, J. Plusquellic, "Measuring Power Distribution System Resistance Variations", *IEEE Transactions on Semiconductor Manufacturing*, Volume 21, Issue 3, Aug. 2008, pp. 444-453.
22. J. Lee, M. Tehranipoor, C. Patel, J. Plusquellic, "Securing Designs Against Scan-Based Side-Channel Attacks", *IEEE Transactions on Dependable and Secure Computing*, Volume 4, Number 4, Oct.-Dec. 2007, pp. 325-336.
23. J. Plusquellic, D. Acharyya, A. Singh, M. Tehranipoor, C. Patel, "Quiescent-Signal Analysis: A Multiple Supply Pad I_{DDQ} Method", *IEEE Design and Test of Computers*, Volume 23, Issue 4, April 2006, pp. 278-293.
24. A. Singh, J. Plusquellic, D. Phatak, C. Patel, "Defect Simulation Methodology for iDDT Testing", *Journal of Electronic Testing, Theory and Applications*, Volume 22, Number 3, June 2006, pp. 255-272.
25. C. Patel, A. Singh, J. Plusquellic, "Defect Detection Using Quiescent Signal Analysis", *Journal of Electronic Testing, Theory and Applications*, Volume 21, Number 5, Oct. 2005, pp. 463-483.
26. S. Kamal Bahl, J. Plusquellic, J. Thomas, "A Comparative Study of W-CDMA Cell Search Designs", *Journal of Circuits, Systems and Computers*, Volume 14, Number 1, Feb. 2005, pp. 129-136.
27. C. Patel, E. Staroswiecki, S. Pawar, D. Acharyya, J. Plusquellic, "Defect Diagnosis using a Current Ratio based Quiescent Signal Analysis Model for Commercial Power Grids", *Journal of Electronic Testing, Theory and Applications*, Volume 19, Number 6, Dec. 2003, pp. 611-623.
28. D. S. Phatak, T. Goff, J. Plusquellic, "IP-in-IP Tunneling to Enable the Simultaneous use of Multiple IP Interfaces for Network Level Connection Striping", *Computer Networks: The International Journal of Computer and Telecommunications Networking*, Volume 43, Issue 6, Dec. 2003, pp. 787-804.
29. J. Plusquellic, A. Singh, C. Patel, A. Gattiker, "Power Supply Transient Signal Analysis for Defect-Oriented Test", *IEEE Transactions on Computer Aided*

Design of Integrated Circuits and Systems, Volume 22, Issue 3, March 2003, pp. 370-374.

30. J. Plusquellic, "IC Diagnosis Using Multiple Supply Pad I_{DDQ}s", *IEEE Design and Test of Computers*, Volume 18, Number 1, Jan. 2001, pp. 50-61.

31. J. Plusquellic, D. M. Chiarulli, S. P. Levitan, "Time and Frequency Domain Transient Signal Analysis for Defect Detection in CMOS Digital ICs", *IEEE Transactions on Circuits and Systems I,* Volume 46, Issue 11, Nov. 1999, pp. 1390-1394.

32. J. Plusquellic, D. M. Chiarulli, S. P. Levitan, "Digital IC Device Testing by Transient Signal Analysis (TSA)", *IEE Electronics Letters*, Volume 31, Issue 18, Aug. 1995, pp. 1568–1570.

Refereed Conference Publications

1. D. Heeger, M. Garigan, E.E. Tsiropoulou, J. Plusquellic, "Secure Energy Constrained LoRa Mesh Network", *AdHocNow*, 2020.
2. K. Rael, G. Fragkos, J. Plusquellic and E. E. Tsiropoulou, " UAV-enabled Human Internet of Things", *Wi-DroIT (Wireless Drones over Internet of Things)*, 2020.
3. D. Heeger and J. Plusquellic, "Analysis of IoT Authentication Over LoRa", *REFRESH*, 2020.
4. G. Fragkos, C. Minwalla, J. Plusquellic, E. E. Tsiropoulou, "Reinforcement Learning Toward Decision-Making for Multiple Trusted-Third-Parties in PUF-Cash", *WFIoT*, 2020.
5. T. J. Mannos, J. Plusquellic, B.Dziki, "Information Leakage Analysis using Accelerated Fault Injection Emulation of a RISC-V Microprocessor", *GOMAC*, 2020.
6. G. Fragkos, C. Minwalla, J. Plusquellic, E.E. Tsiropoulou, "Reinforcement Learning Toward Decision-Making for Multiple Trusted-Third-Parties in PUF-Cash", Invited paper, *WFIoT*, 2020.
7. A. S. Siddiqui, G. Shirley, S. Bendre, G. Bhagwat, J. Plusquellic, F. Saqib, "Secure Design Flow of FPGA Based RISC-V Implementation", *IVSW*, 2019.
8. D. Forte, S. Bhunia, R. Karri, J. Plusquellic, M. Tehranipoor, "IEEE International Symposium on Hardware Oriented Security and Trust (HOST): Past, Present and Future", *ITC*, 2019.
9. A. Siddiqui, Y. Gui, D. Lawrence, S. Laval, J. Plusquellic, M. Manjrekar, B. Chowdhury, F. Saqib, "Hardware Assisted Security Architecture for Smart Grid", *Conference of the IEEE Industrial Electronics Society*, 2018.
10. W. Che, M. Martinez-Ramon, G. Pocklassery, F. Saqib and J. Plusquellic, "Delay Model and Machine Learning Exploration of a Hardware-Embedded Delay PUF", *Symposium on Hardware-Oriented Security and Trust (HOST)*, 2018.
11. G. Pocklassery, W. Che, F. Saqib and J. Plusquellic, "Self-Authenticating

Secure Boot for FPGAs", *Symposium on Hardware-Oriented Security and Trust (HOST)*, 2018.

12. A. S. Siddiqui, C.-C. Lee, W. Che, J. Plusquellic and F. Saqib, "Secure Intra-Vehicular Communication over CANFD", AsianHOST, 2017.
13. G. Pocklassery, Venkata K Kajuruli and F. Saqib, J. Plusquellic, "Physical Unclonable Functions and Dynamic Partial Reconfiguration for Security in Resource-Constrained Embedded Systems", *Symposium on Hardware-Oriented Security and Trust (HOST)*, 2017.
14. A. S. Siddiqui, Y. Gui, J. Plusquellic and F. Saqib, "Secure Communication over CANBus", *International Midwest Symposium on Circuits and Systems (MWSCAS)* , 2017.
15. D. Ismari, C. Lamech, S. Bhunia, F. Saqib and J. Plusquellic, "On Detecting Delay Anomalies Introduced by Hardware Trojans", *International Conference on Computer-Aided Design*, 2016.
16. A. S. Siddiqui, Y. Gui, J. Plusquellic and F. Saqib, "Hardware Based Security Enhanced Framework for Automotive", *Vehicular Networking Conference*, 2016.
17. F. Zhang, S. Bhunia, J. Plusquellic, "Current based PUF Exploiting Random Variations in SRAM Cells", *Design and Automation in Europe (DATE)*, 2016.
18. W. Che, F. Saqib, J. Plusquellic, "PUF-Based Authentication", **Invited Paper**, *International Conference on Computer-Aided Design (ICCAD)*, 2015.
19. I. Wilcox, F. Saqib, J. Plusquellic, "GDS-II Trojan Detection using Multiple Supply Pad V_{DD} and GND I_{DDQ}s in ASIC Functional Units", *Symposium on Hardware-Oriented Security and Trust (HOST)*, 2015.
20. C. Konstantinou, M. Maniatakos, F. Saqib, S. Hu, J. Plusquellic and Y. Jin, "Cyber-Physical Systems: A Security Perspective", *European Test Conference (ETS)*, May, 2015.
21. W. Che, S. Bhunia and J. Plusquellic, "A Non-Volatile Memory based Physically Unclonable Function without Helper Data", *International Conference on Computer-Aided Design*, 2014.
22. D. Ismari and J. Plusquellic, "IP-Level Implementation of a Resistance-Based Physical Unclonable Function", *Symposium on Hardware-Oriented Security and Trust (HOST)*, 2014, pp. 64-69.
23. M. Areno and J. Plusquellic, "Secure Mobile Association and Data Protection with Enhanced Cryptographic Engines", *PRISMS*, 2013.
24. J. Ju, R. Chakraborty, C. Lamech, J. Plusquellic, "Stability Analysis of a Physical Unclonable Function based on Metal Resistance Variations", *Symposium on Hardware-Oriented Security and Trust (HOST)*, 2013, pp. 143-150.
25. J. Aarestad, D. Acharyya, J. Plusquellic, "An Error-Tolerant Bit Generation Technique For Use With A Hardware-Embedded Path Delay PUF", *Symposium on Hardware-Oriented Security and Trust (HOST)*, 2013, pp. 151-158.

26. R. Chakraborty, C. Lamech, D. Acharyya and J. Plusquellic, "A Transmission Gate Physical Unclonable Function and On-Chip Voltage-to-Digital Conversion Technique", *Design Automation Conference*, 2013, pp. 1-10.

27. M. Areno and J. Plusquellic, "Securing Trusted Execution Environments with PUF Generated Secret Keys", *TrustCom*, 2012.

28. J. Ju, R. Chakraborty, R. Rad, J. Plusquellic, "Bit String Analysis of Physical Unclonable Functions based on Resistance Variations in Metals and Transistors", *Symposium on Hardware-Oriented Security and Trust (HOST)*, 2012, pp. 13-20.

29. C. Lamech and J. Plusquellic, "Trojan Detection based on Delay Variations Measured using a High-Precision, Low-Overhead Embedded Test Structure", *Symposium on Hardware-Oriented Security and Trust (HOST)*, 2012, pp. 75-82.

30. C. Lamech, J. Aarestad, J. Plusquellic, R. Rad, K. Agarwal, "REBEL and TDC: Two Embedded Test Structures for On-Chip Measurements of Within-Die Path Delay Variations", *International Conference on Computer-Aided Design (ICCAD)*, 2011, pp. 170-177.

31. C. Lamech, J. Aarestad, K. Agarwal, J. Plusquellic, "Characterizing Within-Die and Die-to-Die Delay Variations Introduced by Process Variations and SOI History Effect", *Design Automation Conference* (*DAC*), 2011, pp. 534-539.

32. J. Plusquellic, D. Acharyya, K. Agarwal, "Measuring Spatial Variation Profile through Power Supply Current Measurements", *International Symposium on Quality Electronic Design* (*ISQED*), 2011, pp. 1-5.

33. K. Agarwal and J. Plusquellic, "Minimally Invasive Methods for Characterizing Within-Die Variation", **(INVITED PAPER)** for Innovative IP Practice session called On-Chip Parametric Sensors, *VLSI Test Symposium*, 2011.

34. D. Acharyya, K. Agarwal, J. Plusquellic, "Leveraging Existing Power Control Circuits and Power Delivery Architecture for Variability Measurement", *International Test Conference*, 2010.

35. J. Plusquellic and D. Acharyya, "Leveraging the Power Grid for Localizing Trojans and Defects", *International Symposium on Testing and Failure Analysis*, 2010.

36. R. Helinski, D. Acharyya, J. Plusquellic, "Quality Metric Evaluation of a Physical Unclonable Function Derived from an IC's Power Distribution System", *Design Automation Conference*, 2010, pp. 240-243.

37. V. Murray, G. A. Feucht, J. C. Lyke, M. Pattichis, J. Plusquellic, "Cell-Based Architecture for Reconfigurable Wiring Manifolds", *American Institute of Aeronautics and Astronautics*, 2010.

38. K. Agarwal, D. Acharyya, J. Plusquellic, "Characterizing Within-Die Variation from Multiple Supply Port I_{DDQ} Measurements", *International Conference on Computer-Aided Design*, 2009, pp. 418-424.

39. R. Helinski, D. Acharyya, J. Plusquellic, "A Physical Unclonable Function Defined Using Power Distribution System Equivalent Resistance Variations", *Design Automation Conference*, 2009, pp. 676 - 681.

40. R. M. Rad, X. Wang, M. Tehranipoor, J. Plusquellic, "Power Supply Signal Calibration Techniques for Improving Detection Resolution to Hardware Trojans", *International Conference on Computer-Aided Design*, Nov., 2008, pp. 632-639.

41. W. Xiaoxiao, S. Hassan Salmani, M. Tehranipoor, J. Plusquellic, "Hardware Trojan Detection and Isolation Using Current Integration and Localized Current Analysis", *International Symposium on Defect and Fault Tolerance in VLSI Systems*, Oct. 2008, pp. 87-95.

42. M. Itskovich, J. Plusquellic, "I_{DDT} Test Calibration Using a Programmable Processing Array", *4th Southern Conference on Programmable Logic*, March, 2008, pp. 265-268.

43. J. Plusquellic, D. Acharyya, M. Tehranipoor, C. Patel, "Triangulating to a Defect's Physical Coordinates Using Multiple Supply Pad IDDQs: Test Chip Results", *International Symposium on Testing and Failure Analysis*, Nov. 2006, pp. 36-45.

44. K. Agarwal, F. Liu, C. McDowell, S. Nassif, K. Nowka, M. Palmer, D. Acharyya, J. Plusquellic, "A Test Structure for Characterizing Local Device Mismatches", *Symposium on VLSI Circuits*, June 2006, pp. 67-68.

45. J. Lee, M. Tehranipoor, J. Plusquellic, "A Low-Cost Solution for Protecting IPs against Scan-Based Side-Channel Attacks", *VLSI Test Symposium*, May 2006, pp. 42-47.

46. N. Ahmed, C. P. Ravikumar, M. Tehranipoor, J. Plusquellic, "At-Speed Transition Fault Testing with Low Speed Scan Enable", *VLSI Test Symposium*, May 2005, pp. 42-47 (**BEST PAPER AWARD**).

47. D. Acharyya, J. Plusquellic, "Hardware Results Demonstrating Defect Detection using Power Supply Signal Measurements", *VLSI Test Symposium*, May 2005, pp. 433-438.

48. J. Lee, M. Tehranipoor, C. Patel, J. Plusquellic, "Securing Scan Design Using Lock and Key Technique", *International Symposium on Defect and Fault Tolerance in VLSI Systems*, Oct. 2005, pp. 51-62.

49. D. Acharyya, J. Plusquellic, "Hardware Results Demonstrating Defect Localization using Power Supply Signal Measurements", *International Symposium on Testing and Failure Analysis*, Nov. 2004, pp. 58-66.

50. A. Singh, C. Patel, J. Plusquellic, "Fault Simulation Model for iDDT Testing: An Investigation", *VLSI Test Symposium*, April 2004, pp. 304-310.

51. A. Singh, C. Patel, J. Plusquellic, "On-chip Impulse Response Generation for Analog and Mixed-signal Testing", *International Test Conference*, Oct. 2004, pp. 262-270.

52. C. Patel, A. Singh, J. Plusquellic, "Defect Detection under Realistic Leakage

Models using Multiple IDDQ Measurements", *International Test Conference*, Oct. 2004, pp. 319-328.

53. A. Singh, J. Tharian, J. Plusquellic, "Path Delay Estimation using Power Supply Transient Signals: A Comparative Study using Fourier and Wavelet Analysis", *International Conference on Computer-Aided Design*, Nov. 2003, pp. 748-753.

54. D. Acharyya, J. Plusquellic, "Impedance Profile of Commercial Power Grid and Test System", *International Test Conference*, Oct. 2003, pp. 709-718.

55. J. Plusquellic, D. Phatak, "Localizing Faults in Digital Chips using Steady-State Current Measurements", *NASA Symposium on VLSI Design*, May 2003.

56. A. Singh, D. S Phatak, T. Goff, M. Riggs, J. Plusquellic, C. Patel, "Comparison of Branching CORDIC Implementations", *International Conference on Application Specific Systems, Architectures and Processors*, June 2003, pp. 215-225.

57. C. Patel, E. Staroswiecki, S. Pawar, D. Acharyya, J. Plusquellic, "Diagnosis using Quiescent Signal Analysis on a Commercial Power Grid", *International Symposium on Testing and Failure Analysis*, Nov. 2002, pp. 713-722.

58. S. K. Bahl, J. Plusquellic, J. Thomas, "Comparison of Initial Cell Search Algorithms for W-CDMA Systems Using Cyclic and Comma Free Codes", *Midwest Symposium on Circuits and System Conference*, Volume 3, Aug. 2002, pp. 192-195.

59. A. Singh, J. Plusquellic, A. Gattiker, "Power Supply Transient Signal Analysis Under Real Process and Test Hardware Models", *VLSI Test Symposium*, May 2002, pp. 357-362.

60. C. Patel, F. Muradali, J. Plusquellic, "Power Supply Transient Signal Integration Circuit", *International Test Conference*, Nov. 2001, pp. 704-712.

61. A. Singh, C. Patel, S. Liao, J. Plusquellic, A. Gattiker, "Detecting Delay Faults using Power Supply Transient Signal Analysis", *International Test Conference*, Nov. 2001, pp. 395-404.

62. C. Patel, J. Plusquellic, "A Process and Technology-Tolerant IDDQ Method for IC Diagnosis", *VLSI Test Symposium*, May 2001, pp. 145-150.

63. J. Plusquellic, A. Germida, J. Hudson, E. Staroswiecki, C. Patel, "Predicting Device Performance From Pass/Fail Transient Signal Analysis Data", *International Test Conference*, Oct. 2000, pp. 1070-1079.

64. A. Germida, J. Plusquellic, "Detection of CMOS Defects under Variable Processing Conditions", *VLSI Test Symposium*, May 2000, pp. 195-201.

65. J. Plusquellic, A. Germida, Z. Yan, "8-bit Multiplier Simulation Experiments Investigating the Use of Power Supply Transient Signals for the Detection of CMOS Defects", *International Symposium on Defect and Fault Tolerance in VLSI Systems*, Nov. 1999, pp. 68-76.

66. A. Germida, Z. Yan, J. Plusquellic F. Muradali, "Defect Detection using Power Supply Transient Signal Analysis", *International Test Conference*, Sept. 1999,

pp. 67-76.

67. J. Plusquellic, D. M. Chiarulli, S. P. Levitan, "Characterization of CMOS Defects using Transient Signal Analysis", *International Symposium on Defect and Fault Tolerance in VLSI Systems*, Nov. 1998, pp. 93-101.

68. J. Plusquellic, D. M. Chiarulli, S. P. Levitan, "Identification of Defective CMOS Devices using Correlation and Regression Analysis of Frequency Domain Transient Signal Data", *International Test Conference*, Nov. 1997, pp. 40-49.

69. J. Plusquellic, D. M. Chiarulli, S. P. Levitan, "Digital Integrated Circuit Testing using Transient Signal Analysis", *International Test Conference*, Oct. 1996, pp. 481-490.

Workshops

1. C. Lamech and J. Plusquellic, "Measuring Regional Delay Variations Using a Mux-D Scan Based Embedded Test Structure", *Design for Manufacurability and Yield Workshop*, June, 2012.

2. H. Salmani, M. Tehranipoor, J. Plusquellic, "A Layout-aware Approach for Improving Localized Switching to Detect Hardware Trojans in Integrated Circuits", accepted *International Workshop on Information Forensics and Security*, 2010.

3. R. M. Rad, J. Plusquellic, C. Patel, A. Singh, "Verification of Convolution Relation Between Sensitized Path's Gate Transients, Power Grid Impulse Responses and Power Port Transients", *D3T Workshop*, co-located with ITC, Nov. 2009.

4. J. Plusquellic, K. Agarwal, D. Acharyya, "Characterizing Within-Die Variation from Multiple Supply Port I_{DDQ} Measurements", *Design for Manufacturability and Yield Workshop*, co-located with DAC, June 2009.

5. H. Salmani, M. Tehranipoor, J. Plusquellic, "New Design Strategy for Improving Hardware Trojan Detection and Reducing Trojan Activation Time", *2nd International Workshop on Hardware-Oriented Security and Trust*, co-located with DAC, June 2009.

6. W. Xiaoxiao, M. Tehranipoor, J. Plusquellic, "Detecting Malicious Inclusions in Secure Hardware: Challenges and Solutions", *1st International Workshop on Hardware-Oriented Security and Trust*, co-located with DAC, June 2008, pp. 15-19.

7. R. Rad, J. Plusquellic, M. Tehranipoor, "Sensitivity Analysis to Hardware Trojans using Power Supply Transient Signals", *1st International Workshop on Hardware-Oriented Security and Trust*, June 2008, pp. 3-7.

8. R. Helinski and J. Plusquellic, "Detecting Small Delay Defects using Self-Relative Timing Bounds", *Defect Based Testing Workshop*, Nov. 2007.

9. R. MohammadPourrad, "Temporal Analysis and Spatial Deconvolution of Power Pad Transients Signals for Fault Localization", *Defect Based Testing Workshop*, Nov. 2007.

10. J. Plusquellic, D. Acharyya, A. Singh, M. Tehranipoor and C. Patel, "Multiple Supply Pad IDDQ-based Defect Detection Techniques Applied to Hardware Test Chips", *Defect Based Testing Workshop*, Nov. 2006.
11. J. Lee, N. Ahmed, M. Tehranipoor, V. Jayaram and J. Plusquellic, "A Novel Framework for Functionally Untestable Transition Fault Avoidance during ATPG", *North Atlantic Test Workshop*, May 2006.
12. J. Plusquellic, D. Acharyya, M. Tehranipoor and C. Patel, "Triangulating to a Defect's Physical Coordinates Using Multiple Supply Pad IDDQs: Test Chip Results", *North Atlantic Test Workshop*, May 2006.
13. N. Ahmed, M. Tehranipoor, C. P. Ravikumar, J. Plusquellic, "At-Speed Transition Fault Testing Using Low Speed Testers with Application to Reduced Signal Enable Routing Area", *North Atlantic Test Workshop*, May 2005.
14. D. Acharyya, A. Singh, M. Tehranipoor, C. Patel and J. Plusquellic, "Sensitivity Analysis of Quiescent Signal Analysis for Defect Detection", *Defect Based Testing Workshop*, May 2005, pp. 3-10.
15. D. Acharyya and J. Plusquellic, "Calibrating Power Supply Signal Measurements for Process and Probe Card Variations", *Defect Based Testing Workshop*, April 2004, pp. 23-30.
16. C. Patel, E. Staroswiecki, D. Acharyya, S. Pawar, and J. Plusquellic, "A Current Ratio Model for Defect Diagnosis using Quiescent Signal Analysis", *Defect Based Testing Workshop*, April 2002.
17. J. Plusquellic, C. Patel, and Y. Ouyang, "Quiescent Signal Analysis for IC Diagnosis", *System Test and Diagnosis Workshop,* Oct. 2000.
18. J. Plusquellic, D. M. Chiarulli, and S. P. Levitan, "An Automated Technique to Identify Defective CMOS Devices based on Linear Regression Analysis of Transient Signal Data", *Workshop on I_{DDQ} Testing*, Nov. 1998, pp. 32-36.

Invited Talks, Seminars and Tutorials

1. "2nd Working Group Meeting on Logic Locking & Anti-Trojan Solutions", *invited participant*, Organized by Jeyavijayan Rajendran Texas A&M, Jin Yier and Swarup Bhunia, Univ. of Florida on behalf of DARPA, Nov. 2019.
2. "Trust and Security Opportunities and Challenges in Hardware Security", Jim Plusquellic, Swaroop Ghosh, Rashmi Jha, *NSF PI meeting*, Oct. 2019.
3. "Quantifiable Assurance using Hardware Primitives and Reconfiguration", Invited talk, *Office of Secretary of Defense*, Oct. 2019.
4. "Hardware Security and Trust", Invited talk, *DOD* at UNM, Sept. 2019.
5. "Hardware-Oriented Security and Trust", *Research Spotlight Forum on CyberSecurity*, *Sandia National Laboratories,* Aug. 2019.
6. "1st Working Group Meeting on Logic Locking & Anti-Trojan Solutions", *invited participant*, Organized by Jeyavijayan Rajendran Texas A&M, Jin Yier and Swarup Bhunia, Univ. of Florida on behalf of DARPA, June 2019.

7. "Side Channel Analysis and Countermeasures", *HOST Tutorial*, May, 2019.
8. "Authentication using Physical Unclonable Functions for Secure Tactical Communications", *Army Research Laboratory*, Aug., 2018.
9. "Hardware Embedded Delay PUF", *Govt. contractor*, July, 2018.
10. "PUF-Based Authentication and Secure Boot for IoT", *HOST Tutorial*, May, 2018.
11. "Authentication using Physical Unclonable Functions for Secure Tactical Communications", *Army Research Laboratory*, Aug., 2018.
12. "Hardware-Oriented Security and Trust", *Central Intelligence Agency*, Jan. 2018.
13. "Hardware-Based Security and Trust For IoT and Supply Chain Authentication", *Georgia Tech Invited presentation*, April, 2017.
14. "A Hardware-Embedded Delay PUF (HELP) for IoT and Supply Chain Security Challenges", *Enthentica lunch presentation at HOST*, May, 2017.
15. "Hardware Security and Trust Challenges in Emerging IoT Systems and Applications", *HOST Tutorial,* May 2017.
16. "Hardware-Based Techniques for Securing the Supply Chain and Validating Chip Functionality", *Army Research Laboratory*, 2017.
17. "Supply Chain Authentication", *Sandia National Labs*, Jan. 2017.
18. "Research Overview", *Air Force Research Laboratory*, 2016.
19. "PUF-Based Authentication", Invited presentation, Nov. 2015.
20. "Hardware Primitives for Trusted and Secure Systems", Distinguished talk, *Florida Institute of Technology,* Nov. 2014.
21. "Hardware Primitives for Trusted and Secure Systems", Invited talk, *University of South Florida,* Nov. 2014.
22. "Hardware Primitives for Trusted and Secure Systems", Invited talk, *University of Central Florida,* Nov. 2014.
23. "Hardware Primitives for Trusted and Secure Systems", Invited talk, *Sandia National Laboratories,* Nov. 2014.
24. "An Embedded Test Structure for Improving Yield Learning, Profiling New Product Introductions, and Implementing Hardware Security Primitives", Invited talk, *Intel FSM College of Engineering, Technical Seminar Series,* March 2013.
25. "Physical Unclonable Functions and Embedded Test Structures for Hardware-Based Security and Design for Manufacturability", Invited talk, *Arizona State University*, Feb. 2013.
26. "DFT and ATE Working Together to Tackle Next Generation Yield Learning Challenges", Invited talk, *Verigy*, Nov., 2011.
27. "A Truly Embedded Test Structures for Measuring Path Delay Variations in Integrated Circuits", Invited talk, *NVidia*, Nov., 2011.

28. Cyber Security Forum at Sandia, "Power Grid PUF: A Physical Unclonable Function Based on Power Grid Resistance Variations", Invited talk, *Sandia National Laboratories*, Oct. 2011.
29. University Partners, Cyber Open House and Workshop, invitee, Invited talk, *Sandia National Laboratories*, July, 2011.
30. "Power Grid Physical Unclonable Function and Change Detection using Regional Side Channel Analysis", Invited talk, *DARPA*, 2011
31. "Truly Embedded Test Structures for Measuring Power and Delay Variations in Integrated Circuits", Invited talk, *QualComm*, June, 2011.
32. "Minimally Invasive Methods for Characterizing Within-Die Variation", K. Agarwal, D. Acharyya and J. Plusquellic, **INVITED PAPER AND TALK** for Innovative IP Practice session called On-Chip Parametric Sensors, *VLSI Test Symposium*, 2011.
33. "Addressing Process Variability Challenges through better Coupling between Design and Technology", K. Agarwal and J. Plusquellic , **INVITED TALK**, *Design for Reliability and Variability Workshop*, 2011.
34. "Emerging Hardware-Oriented Security and Trust Issues in the Design and Fabrication of Integrated Circuits", **INVITED TALK**, *VLSI Test Symposium*, 2011.
35. "FPGA Applications: From Embedded System Design to Hardware Security and Trust", Invited talk, *Honeywell*, Oct, 2010.
36. "Change Detecting using Regional Power Signal (Side-Channel) Analysis Methods", *Analytical Solutions Inc.* and *DARPA*, Sept, 2010.
37. "Leveraging the Power Grid for Applications in Hardware Security and Trust", *ECE Graduate Seminar*, Sept, 2010.
38. "Experimental Analysis of Regional Leakage and Delay Variations", Invited talk, *NVIDIA*, July, 2010.
39. "Hot Topics in Hardware-Oriented Security and Trust", Invited talk, *Sandia National Laboratory*, July, 2010.
40. "How Much Can I Trust the IC and Hardware?", **INVITED TALK**, *NASA/ ESA Conference on Adaptive Hardware and Systems*, June, 2010.
41. "A Non-Destructive IC Change Detection Method", Invited talk, *Analytical Solutions Inc.*, May, 2010.
42. "A Power Grid Physical Unclonable Function", Invited talk, *UNM Science and Technology Center*, May, 2010.
43. "Design for Manufacturability: Embeddable Test Structures for Measuring Process Variations and Assessing DFM Practice", Invited talk, *IBM ARL*, Nov., 2009.
44. "Design for Manufacturability: Embeddable Test Structures for Measuring Process Variations and Assessing DFM Practice", Invited talk, *Univ. of Texas, Austin*, Nov., 2009.

45. "Leveraging the Power Grid for Applications in Hardware Security and Trust", Invited talk, *ARO Workshop*, Aug., 2009.
46. "Hardware Security: Test Constraints and Implications for ATE", Invited talk, Quarterly Research and Innovation Forum, *Verigy*, July, 2009.
47. "Design for Manufacturability: Embeddable Test Structures for Measuring Process Variations and Assessing DFM Practice", Invited talk, *NVIDIA*, July, 2009.
48. "Leveraging the Power Grid for Applications in Hardware Security and Trust", *Faculty Research Colloquium*, Mar. 2009.
49. "Leveraging the Power Grid for Applications in Hardware Security and Trust", *ECE Graduate Seminar*, Jan. 2009.
50. "Leveraging the Power Grid for Applications in Hardware Security and Trust", *Sandia National Laboratory*, Jan. 2009.
51. "Leveraging the Power Grid for Applications in Hardware Security and Trust", *Microelectronics Research and Development Corporation*, Jan. 2009.
52. "PUFs and Trojan Detection for Hardware Security", *Air Force Research Laboratory*, Dec. 2008.
53. "PUFs and Trojan Detection for Hardware Security", *Air Force Research Laboratory*, Nov. 2008.
54. "Physically Unclonable Functions Derived from Power Grid Resistance Variations", *Xilinx*, Nov. 2008.
55. "Trojan Circuit Detection Techniques and Design for Manufacturability", *Faculty Candidate Interview at University of New Mexico*, May, 2008.
56. "Power Supply Testing Methods for Defect Detection and Identification of Malicious Circuit Inclusions", Invited talk, *CSEE Research Review at UMBC*, May 2007.
57. "Challenges and Solutions to Screening Defective Chips in Nanometer Technologies", Invited talk, *QualComm*, Jan. 2007.
58. "A Solution for Continued Use of I_{DDQ} in DSM Technologies", Invited talk, *NVIDIA*, Nov. 2006.
59. "An RC Test Infrastructure for Monitoring BEOL Process Variations", Seminar, *IBM Austin Research Laboratory*, May 2004.
60. "Defect-Based Test for Defect Detection and Localization", Invited talk, *University of Texas at Austin*, March 2004.
61. "Hardware Results Demonstrating Fault Localization Using Power Supply Signal Measurements", Invited talk and paper, *IBM Austin Center for Advanced Studies Conference*, Austin Research Labs, Feb. 2004.
62. "I_{DDX}-based Fault Localization", Invited talk and paper, *IBM Austin Center for Advanced Studies Conference*, Austin Research Labs, Feb. 2003.
63. "A Current Ratio Model for Defect Diagnosis using Quiescent Signal

Analysis", Invited talk and paper, *IBM Austin Center for Advanced Studies Conference*, Austin Research Labs, Feb. 2002.

64. "I_{DDX}-based Testing Methods for Defect Detection, Diagnosis and Performance Characterization", Invited seminar, *Case Western Reserve University*, Nov. 2001.
65. "Multiple Power Supply Pad V_{DDT} Testing for Delay Faults", Invited talk and paper, *IBM Austin Center for Advanced Studies Conference*, Austin Research Labs, Feb. 2001.
66. "Static and Dynamic IDD Methods for Testing, Diagnosing and Estimating Performance of Deep Sub-micron Digital Integrated Devices", Invited talk, *Intel's Manufacturing Test Research Symposium*, Aug. 2000.
67. "The Linux Operating System", Invited talk, *Johns Hopkins Applied Physics Laboratory*, July 2000.
68. "Sharing Good Test Ideas", Invited presentation at IBM in Berlington, May 2000.
69. "Computer Architecture", Invited tutorial, *Texas A&M*, June 1999.
70. "VLSI Design", Invited tutorial, *Texas A&M*, April 1999.
71. "Detecting Fabrication Defects in Digital Integrated Circuits Using Transient Signal Analysis," Invited talk, *Design Technology Center at Hewlett-Packard*, Nov. 1998.
72. "Applications of Transient Signal Analysis for CMOS Defect Detection and Failure Analysis," Invited talk, *University of Pittsburgh*, Oct. 1998.
73. "Digital Integrated Circuit Device Testing using Transient Signal Analysis," Invited talk, *Laboratory of Physical Sciences*, University of Maryland, College Park, Feb. 1998.
74. "Digital Integrated Circuit Device Testing using Transient Signal Analysis," Invited talk, *DOD*, Oct. 1997.
75. "Time and Frequency Domain Transient Signal Analysis for Defect Detection in CMOS Digital ICs," Invited talk, *Center for Reliable Computing at Stanford University*, Hosted by Professor Edward J. McCluskey, Nov. 1996.
76. "Time and Frequency Domain Transient Signal Analysis for Defect Detection in CMOS Digital ICs," Invited talk, *Design Technology Center at Hewlett-Packard*, Nov. 1996.
77. "Programming in X Windows, from Xlib to Motif," Tutorial, *University of Pittsburgh*, May 1993.
78. "Neural Network Architectures and Algorithms," Tutorial, *University of Pittsburgh*, March 1992.

Patents

Patent 10,409,274, "Control System Backplane Monitoring with FPGA", collaboration with Sandia National Laboratories, Sept. 2019.

Patent 10,366,253, “Reliability enhancement methods for physically unclonable function bitstring generation”, July, 2019.

Patent 10,230,369, “Systems and methods for leveraging path delay variations in a circuit and generating error-tolerant bitstrings”, March 2019.

Patent 10,216,965, “Systems and Methods for Generating Physically Unclonable Functions from Non-Volatile Memory Cells”, Feb. 2019.

Patent 10,048,939. Systems and Methods for Analyzing Stability using Metal Resistance Variations, August 14, 2108.

Patent 9,030,226 ,“System and Methods for Generating Unclonable Security Keys in Integrated Circuits, May 15, 2015.

Patent 8,610,454, “System and Methods for Generating Unclonable Security Keys in Integrated Circuits”, December 17, 2013.

Patent 7,622,942, “Method and Apparatus for Measuring Device Mismatches”, November 24, 2009.

Patent 7,408,372, “Method and Apparatus for Measuring Device Mismatches”, August 5, 2008.

Patent 7,043,389, “Method and System for Identifying and Locating Defects in an Integrated Circuit”, May 9, 2006.

Provisionals

“PUF-based Authentication for Resource Constraint Environments (PARCE)”, March, 2020 (licensed to IC-Safety, LLC).

“System and Methods for Entropy and Statistical Quality Metrics in Physical Unclonable Function Generated Bitstrings”, August 29, 2019 (licensed to Enthentica, Inc.).

“Systems and Methods for Leveraging Path Delay Variations in a Circuit and Generating Error-Tolerant Bitstrings”, March 21, 2019 (licenced to Enthentica, Inc.).

“A Privacy-Preserving, Mutual PUF-based Authentication Protocol”, Jan. 2019 (licensed to Enthentica, Inc.).

“System and Methods for Analyzing Stability Using Metal Resistance Variations”, Aug. 17, 2013 (licensed by IC-Safety, LLC).

“Correlation-Based Robust Authentication”, July, 2018 (licensed to IC-Safety, LLC).

“Autonomous, Self-Authenticating and Self-Contained Secure Boot Process for FPGAs”, Jan, 2018 (licensed by Enthentica, Inc.).

“Reliability Enhancement Methods for Physically Unclonable Function Bitstring Generation”, Dec. 2017 (licensed to Enthentica, Inc.).

"Side-channel Power Resistance for Encryption Algorithms using Dynamic Partial Reconfiguration (SPREAD)", Oct. 2017 (licensed by IC-Safety, LLC)

"Novel Methods designed to improve Entropy and Statistical Quality metrics in PUF generated bitstrings", Nov. 2016 (licensed by Enthentica, Inc.).

"Control System Backplane Monitoring with FPGA", collaboration with Sandia National Laboratories, Aug. 2016.

"PUF Authentication Protocols", Jan. 2016 (licensed by Enthentica, Inc.).

"Voltage-Based-Enrollment for Improving the Reliability of Physical Unclonable Functions", Dec. 2014, (licensed by Enthentica, Inc.).

"IP-Level Implementation of a Resistance-Based Physical Unclonable Function", June, 2014 (licensed by IC-Safety, LLC).

"Physical Unclonable Function Built from Non-Volatile Memory Cells", Dec. 2013, (licensed by IC-Safety, LLC).

"Systems and Methods for Leveraging Path Delay Variations in a Circuit and Generating Error-Tolerant Bitstrings", Aug. 17, 2013 (licensed by Enthentica, Inc.).

Service

Professional Service

2020	**HOST Covid-19 Panel Organizer and Participant**, HOST webinar, July 2020.
2020-2021	**Program Chair**, International Symposium on Hardware-Oriented Security and Trust (HOST)
2019	HOST, best paper selection committee, chair
2018-present	Editor-in-Chief, Hardware Security Section, Cryptography, MDPI
2017-2018	Associate Editor, Cryptography, MDPI
2016-2017	**Hardware Demonstration Chair**, International Symposium on Hardware-Oriented Security and Trust (HOST)
2017	TPC, Great Lakes Symposium on VLSI
2014	NSF panel
2013	TPC, Design and Test in Europe
2012-2013	Registration Chair, International Symposium on Hardware-Oriented Security and Trust (HOST)
2013	NSF panel
2011	NSF panel
2011-2015	Associate Editor, Transactions on Computers

2011-present	TPC, International Symposium on Hardware-Oriented Security and Trust (HOST)
2010	NSF panel
2010-2012	TPC, ATE Vision 2020
2010	**General Chair**, International Symposium on Hardware-Oriented Security and Trust (HOST)
2009	Progam Chair, HOST
2008	**Program Chair** and **Publication Chair**, International Workshop on Hardware-Oriented Security and Trust (HOST). Mohammad Tehranipoor and I co-founded this workshop
2008-present	Steering Committee, Hardware-Oriented Security and Trust (HOST)
2008	Organizer of the Thesis Research Poster Session at VLSI Test Symposium
2008-2009	Steering Committee, Defect and Data Driven Testing Workshop at the International Test Conference
2007-2009	TPC, International Conference on Computer-Aided Design (ICCAD)
2007	Vice-Program Chair for Defect-Based Testing Workshop at the International Test Conference
2006	General Chair for Defect-Based Testing Workshop at the International Test Conference
2005-2009	TPC, VLSI Test Symposium (VTS)
2005	Program Vice-Chair for Defect-Based Testing Workshop at VLSI Test Symposium
2004	Program Chair for Defect-Based Testing Workshop at VLSI Test Symposium
2003	Program Co-chair for Defect-Based Testing Workshop at VLSI Test Symposium
2002-2011	TPC, International Test Conference (ITC)
	NSF panel member (CISE/CCR/DA)
1999-2003	University Booth Coordinator on SIGDA Advisory Board, ACM

Departmental Service

2018-2019	P&T Committee, CMPE Univ. of New Mexico
2017-present	Area Chair, CMPE Univ. of New Mexico
2017-2018	Faculty Search Committee, CMPE Univ. of New Mexico

2015-2016	Area Chair, CMPE Univ. of New Mexico
2015-2016	Space Committee, Univ. of New Mexico
2013-2014	Computer IT Committee
2013-2014	Space Committee
2010-2011	Area Chair (1.5 years, Aug 2010 through Jan. 2012), CMPE Univ. of New Mexico
2010	Faculty Search Committee, Univ. of New Mexico
2009	Undergraduate Program Committee, Univ. of New Mexico
2008	Graduate Program Committee, Univ. of New Mexico
2008-ongoing	Computer Engineering Committee
2007	Publicity Committee, Univ. of Maryland, Balt. Co. Redeveloping college and department level websites, to improve the process of recruiting high quality CMPE undergraduate students.
2007	Faculty Search Committee
2004-2007	Graduate Program Director in Computer Engineering
2002-2003	Graduate Program Director in Computer Engineering
2002	Course scheduling committee
1999-2012	Computer Engineering Graduate Committee Co-authored graduate program proposal submitted to the Maryland Higher Educational Commission for approval in 2001.
1997-2004	Computer Engineering Undergraduate Committee Attended ABET workshop in May 1999.
1997-2004	Faculty Search Committee
1997-2003	Comprehensive Exam Writing and Grading
1997-2001	Equipment Committee Ordered equipment and configured our test and measurement laboratory for the CMPE undergraduate and graduate programs. Successfully solicited for donations from Tektronics and Xilinx in the amount of ~$100K.
1997-Present	Graduate Admissions

New Course Development: Undergraduate

ECE 443/338 Hardware Design with VHDL/Immediate Logic Design

CMPE 415 Programmable Logic Devices

CMPE 310 Systems Design and Programming

CMPE 413 Principles of VLSI Design

CMPE 414, VLSI Design II

New Course Development: Graduate

ECE 595 VLSI Synthesis

ECE 525 Hardware-Oriented Security and Trust, (2018 created fully on-line version with screencasts)

ECE 522 Hardware-Software Codesign, (2017 created fully on-line version with screencasts)

CMPE 650 Digital Systems Design

CMPE 646 VLSI Design Verification and Testing

CMPE 640 Advanced VLSI Design

CMPE 641 Topics in VLSI

I applied for MOSIS chip fabrication money for the VLSI design courses over the period from 1998-2011 and supervised student testing of fabricated devices. In 2011, we built a 2 mm X 2 mm chip under a MOSIS research contract in IBM's 90 nm technology.

Conference and Journal Referee

MDPI, DATE, HOST, ITC, VTS, ICCAD, DAC, Trans. on VLSI, Trans. on Circuits and Systems, Trans. on Computer-Aided Design, Trans. on Design Automation of Electronic Systems, NATW, DBT, JETTA, Transactions on Instrumentation and Measurement, Transactions on Information Security and Forensics

Memberships

- IEEE, 1995-Present
- ACM, 1997-2003
- Test Technology Technical Committee (TTTC), 1997-2010