Daniel Holcomb

Contact Information

309F Knowles Engineering Building
151 Holdsworth Way
Amherst, MA 01003-9284

holcomb@engin.umass.edu
(413) 545-6593
http://people.umass.edu/dholcomb/

Research Interests

Embedded Systems Security, Applied Formal Methods, Physical Unclonable Functions

Education

UC Berkeley, Berkeley, CA USA

Ph.D., EECS, December 2013

- Dissertation: *Formal Verification and Synthesis for Quality-of-Service in On-Chip Networks*
- Adviser: Sanjit A. Seshia, EECS
- Major: Design of Electronic Systems
- Minors: VLSI; Industrial Engineering and Operations Research

UMass Amherst, Amherst, MA USA

M.S., ECE, September 2007

- Thesis: *Chip ID and True Random Number Generation*
- Adviser: Wayne P. Burleson, ECE

B.S., ECE, *Summa Cum Laude,* September 2005

- Thesis: *Payload Design for Atmospheric Research Balloon*
- Adviser: Paul B. Voss, Geosciences

Academic Appointments

UMass Amherst, Amherst, MA USA
Associate Professor **Jan 2021 - Present**
Assistant Professor **Jan 2015 - Jan 2021**

University of Michigan, Ann Arbor, MI USA
Research Fellow **Oct 2013 - Dec 2014**

UC Berkeley, Berkeley, CA USA
Graduate Student Researcher **Spring 2007 - Summer 2013**

UMass Amherst, Amherst, MA USA
Graduate Research Assistant, ECE **Fall 2005 - Summer 2007**
Undergraduate Research Assistant, Atmospheric Research Lab **Summer 2004 - Summer 2005**

Smith College, Northampton, MA USA
Consultant, Atmospheric Research Lab **Fall 2005**

Industry Appointments

Amida Technology Solutions, Washington, DC USA
Consultant **Nov 2019 - Nov 2021**

Virta Labs, Ann Arbor, MI USA
Hardware Engineering Lead **Jan 2014 - Dec 2015**
Embedded systems research and development at security startup

Intel, Hillsboro, OR USA
Technology Transfer Intern – Strategic CAD Lab **Summer 2011; Summer 2012 - Spring 2013**
Microarchitectural synthesis and formal verification for on-chip networks

Intel, Hudson, MA USA
Graduate Technical Intern **Spring-Summer 2006; Summer 2007**
Analysis and mitigation of particle-strike induced errors in combinational circuits and memories

Teaching

UMass Amherst, Amherst, MA USA

ECE697RD: Hardware Security **Spring 2022**
Special topics course covering intersection of VLSI and security, including circuits for PUFs, TRNGs, Trojans, and tools for reverse engineering from layout.

ECE622: Modeling and Verification of Embedded Systems **Spring 2015/6/7/8/9/20/1/2**
Mezzanine level embedded systems course using Lee and Seshia textbook. Labs focus on reachability analysis of FSMs, and timed/hybrid automata.

ECE558/658: VLSI Design **Fall 2019/20/1**
Introduction to VLSI Design using Weste & Harris textbook. Heavy lab component using industrial tools for circuit simulation, layout, synthesis, and place & route.

ECE591CF: Cybersecurity Lecture Series **Fall 2015/6/8/9**
Co-organized 1-credit seminar course featuring weekly guest speakers

ECE353: Computer Systems Lab **Fall 2015/6/7/8**
Undergraduate course on applied embedded systems. Prototyping systems on breadboards using Verilog (Altera CPLD) and C programming (ATmega32)

ECE296/ECE396: Embedded Capture The Flag Competition (Independent Study) **Spring 2016/7**
Organized and supervised team of undergraduate CS and ECE students in semester-long hacking competition conducted by MITRE (18 students participated for credit over the two years).

Senior Design Project **2015/6/7/8/9/20/1**
Supervised undergraduate teams on their year-long design projects

ECE696: Independent Study
- Mohammad Waquas Usmani, Spring 2022
  "Benchmark multiple SMT Solvers to compare Runtime"
- Aleksa Deric, Spring 2020
  "Evaluation of Time-to-digital converter circuits on Xilinx FPGAs"
- Suraj Rao, Spring 2019
  "Design, Implementation and Evaluation of True Random Number Generator on Amazon F1"
- Peter Stanwicks, Spring 2019
  "Threshold Biasing of SRAM for the Storage of Secret Codes"
- Harshavardhan Ramanna, Fall 2017
  "Hardware Design for Test Chip Evaluation of Bitline PUF"
- Mohammad Aftab Usmani, Spring 2016
  "Evaluation of the feasibility of implementing Anderson PUF using SLICE-L cells on Virtex 7 FPGA"
- Abhinav Khandelwal, Fall 2015
  "Design Space Exploration of Error Correction Techniques for Physical Unclonable Functions"

ECE499: Capstone Honors Project
Supervised year-long capstone project of Commonwealth College students
- Richard Hartnett (2018)
  "Evaluation of Security of AES-128 WDDL Implementation on FPGA"
- Thomas Baim (2018)
  "Image Processing and Phone Application Development for Mobile Phone Microscopy and Microfluidics"
- Omid Meh (2016):
  "Automated Mussel Detection Using Mobile Phone Microscopy and Microfluidic Techniques"

Publications

Bold font in author listing denotes students for which I am the primary or co-primary research adviser.

Book Chapters

[1] D Holcomb "Nanoscale CMOS Memory-based Security Primitive Design", Book chapter in: *Security Opportunities in Nano Devices and Emerging Technologies, M. Tehranipoor, D. Forte, G. Rose, S. Bhunia (Eds.), Publisher: CRC Press/Taylor & Francis*, 2017.

Peer-Reviewed Journal Articles

[1] **A. Deric**, and D. Holcomb "Know Time to Die: Integrity Checking for Zero Trust Chiplet-based Systems Using Between-Die Delay PUFs", *IACR Transactions on Cryptographic Hardware and Embedded Systems (CHES)*, 2022. (to appear)

[2] **X. Li**, **P. Stanwicks**, G. Provelengios, R. Tessier, and D. Holcomb "Jitter-based Adaptive True Random Number Generation for FPGAs in the Cloud", *ACM Transactions on Reconfigurable Technology and Systems*, 2022 (to appear)

[3] X. Shao, Z. Chen, D. Holcomb, and L. Gao "Accelerating BGP Configuration Verification through Reducing Cycles in SMT Constraints", *IEEE/ACM Transactions on Networking*, 2022 (to appear)

[4] S. Moini, S. Tian, D. Holcomb, J. Szefer and R. Tessier "Power Side-Channel Attacks on BNN Accelerators in Remote FPGAs", *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, pp 357-370, June 2021.

[5] G Provelengios, D Holcomb, R Tessier, "Mitigating Voltage Attacks in Multi-Tenant FPGAs" *ACM Transactions on Reconfigurable Technology and Systems*, Feb. 2021

[6] **S N Dhanuskodi**, **S Allen**, D Holcomb "Efficient Register Renaming Architectures for 8-bit AES Datapath at 0.55 pJ/bit in 16-nm FinFET", *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, pp 1807-1820, June 2020.

[7] G Provelengios, D Holcomb, R Tessier, "Power Distribution Attacks in Multitenant FPGAs", *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, June 2020.

[8] **MA Usmani**, **S Keshavarz**, E Matthews, L Shannon, R Tessier, D Holcomb "Efficient PUF-Based Key Generation in FPGAs using Per-Device Configuration", *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, Feb. 2019.

[9] N. K. Dumpala, S. B. Patil, D. Holcomb, and R. Tessier, "Loop Unrolling for Energy Efficiency in Low-Cost FPGAs" *ACM Transactions on Reconfigurable Technology and Systems*, Jan. 2019

[10] H Jiang, C Li, R Zhang, P Yan, P Lin, Y Li, JJ Yang, D Holcomb, Q Xia "A Provable Key Destruction Scheme Based on Memristive Crossbar Arrays", *Nature Electronics*, Oct 12 2018.

[11] X Xu, **S Keshavarz**, D Forte, M Tehranipoor, D Holcomb "Bimodal Oscillation as a Mechanism for Autonomous Majority Voting in PUFs", *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, pp 2431 - 2442, Aug. 2018.

[12] **S Keshavarz**, C Yu, S Ghandali, X Xu, D Holcomb "Survey on Applications of Formal Methods in Reverse Engineering and Intellectual Property Protection", *Journal of Hardware and Systems Security*, pp 1-11, Aug. 2018.

[13] A Shanmugam, **M Usmani**, A Mayberry, DL Perkins, DE Holcomb "Imaging systems and algorithms to analyze biological samples in real-time using mobile phone microscopy", *PloS one*, Mar. 2018.

[14] R Zhang, H Jiang, ZR Wang, P Lin, Y Zhuo, D Holcomb, DH Zhang, JJ Yang, Q Xia "Nanoscale diffusive memristor crossbars as physical unclonable functions", *Nanoscale*, pp 2721-2726, Jan. 2018.

[15] **SN Dhanuskodi**, D Holcomb, "Techniques to Reduce Switching and Leakage Energy in Unrolled Block Ciphers", *IEEE Transactions on Computers*, Aug. 2017.

[16] C. Yu, **X. Zhang**, **D. Liu**, M. Ciesielski, D. Holcomb, "Incremental SAT-based Reverse Engineering of Camouflaged Logic Circuits", *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, pp 1647-1659, Jan. 2017

[17] A. Vijayakumar, V.C. Patil, D.E. Holcomb, C. Paar, S. Kundu, "Physical Design Obfuscation of Hardware: A Comprehensive Investigation of Device and Logic-Level Techniques", *IEEE Transactions on Information Forensics and Security (TIFS)*, pp 64-77, Aug. 2016

[18] J. Hester, N. Tobias, A. Rahmati, L. Sitanayah, D. Holcomb, K. Fu, W.P. Burleson, J. Sorber. "Persistent Clocks for Batteryless Sensing Devices", *ACM Trans. Embed. Comput. Syst. 15, 4, Article 77*, pp 1-28, Aug. 2016

[19] X. Xu, A. Rahmati, D. Holcomb, K. Fu, W. Burleson "Reliable Physical Unclonable Functions using Data Retention Voltage of SRAM Cells", *Transactions on Computer-Aided Design of Integrated Circuits and Systems*, pp 903-914, Jun. 2015

[20] D. Holcomb, S. Seshia, "Compositional Performance Verification of NoC Designs", *Transactions on Computer-Aided Design of Integrated Circuits and Systems*, pp 1370-1383, Sep. 2014

[21] R. A. Zaveri, P. B. Voss, C. M. Berkowitz, E. Fortner, J. Zheng, R. Zhang, R. J. Valente, R. L. Tanner, D. Holcomb, T. P. Hartley, L. Baran, "Overnight atmospheric transport and chemical processing of photochemically aged Houston urban and petrochemical industrial plume", *Journal of Geophysical Research: Atmospheres*, Dec. 2010.

[22] D. E. Holcomb, W. P. Burleson, and K. Fu, "Power-Up SRAM State as an Identifying Fingerprint and Source of True Random Numbers" *IEEE Transactions on Computers*, pp 1198 - 1210, Sept. 2009.

[23] E.E. Riddle, P.B. Voss, A. Stohl, D. Holcomb, D. Maczka, K. Washburn, R.W. Talbot, "Trajectory model validation during ICARTT-2004 using newly developed altitude-controlled meteorological balloons", *Journal of Geophysical Research: Atmospheres*, Dec. 2006.

Peer-Reviewed Paper in Conference or Workshop Proceedings

[1] **A. Deric**, and D. Holcomb "Know Time to Die: Integrity Checking for Zero Trust Chiplet-based Systems Using Between-Die Delay PUFs", *IACR Transactions on Cryptographic Hardware and Embedded Systems (CHES)*, 2022

[2] **X. Li**, R. Tessier, D. Holcomb "Precise Fault Injection to Enable DFIA for Attacking AES in Remote FPGAs", *2022 IEEE 30th Annual International Symposium on Field-Programmable Custom Computing Machines (FCCM)*,2022

[3] S. Tian, S. Moini, A. Wolnikowski, D. Holcomb, R. Tessier, J. Szefer "Remote Power Attacks on the Versatile Tensor Accelerator in Multi-Tenant FPGAs", *2021 IEEE 29th Annual International Symposium on Field-Programmable Custom Computing Machines (FCCM)*, 2021

[4] S. Moini, S. Tian, D. Holcomb, J. Szefer, R. Tessier "Remote power side-channel attacks on BNN accelerators in FPGAs", *Design, Automation & Test in Europe (DATE)*, 2021

[5] **X Li**, **P Stanwicks**, G Provelengios, R Tessier, D Holcomb, "Jitter-based Adaptive True Random Number Generation for FPGAs in the Cloud", *International Conference on Field Programmable Technology*, 2020 acceptance rate = 25% (21/83)

[6] S Moini, **X Li**, **P Stanwicks**, G Provelengios, W Burleson, R Tessier, D Holcomb, "Understanding and Comparing the Capabilities of On-Chip Voltage Sensors against Remote Power Attacks on FPGAs", *2020 IEEE 63rd International Midwest Symposium on Circuits and Systems (MWSCAS)*, pp 941-944, 2020

[7] **S N Dhanuskodi**, **X Li**, D Holcomb, "COUNTERFOIL: Verifying Provenance of Integrated Circuits using Intrinsic Package Fingerprints and Inexpensive Cameras", *USENIX security 2020*, 2020 acceptance rate = 17% (44/256)

[8] G Provelengios, D Holcomb, R Tessier, "Power wasting circuits for cloud FPGA attacks", *2020 30th International Conference on Field-Programmable Logic and Applications (FPL)*, pp 231-235, 2020

[9] **S N Dhanuskodi**, D Holcomb, "Enabling Microarchitectural Randomization in Serialized AES Implementations to Mitigate Side Channel Susceptibility", *International Symposium on VLSI (ISVLSI)*, pp 314-319, 2019 [**First Place Best Poster Award**]

[10] G Provelengios, D Holcomb, R Tessier, "Characterizing Power Distribution Attacks in Multi-User FPGA Environments", *Proceedings of the International Conference on Field Programmable Logic and Applications*, pp 194-201, 2019 acceptance rate = 19% (28/151) [**Best Paper award**]

[11] G Provelengios, **C Ramesh**, S B Patil, K Eguro, R Tessier, D Holcomb, "Characterization of Long Wire Data Leakage in Deep Submicron FPGAs", *Proceedings of the 2019 ACM/SIGDA International Symposium on Field-Programmable Gate Arrays*, pp 292-297, 2019

[12] **S Keshavarz**, F Schellenberg, B Richter, C Paar, D Holcomb, "SAT-based Reverse Engineering of Gate-Level Schematics using Fault Injection and Probing", *IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pp 215-220, 2018. [**First Place Best Poster Award**]

[13] **C Ramesh**, S Patil, **SN Dhanuskodi**, G Provelengios, S Pillement, D Holcomb, R Tessier, "FPGA Side Channel Attacks without Physical Access", *IEEE International Symposium on Field-Programmable Custom Computing Machines (FCCM)*, pp 45-52, April 2018. acceptance rate = 21% (22/106)

[14] **S Keshavarz**, D Holcomb "Threshold-based Obfuscated Keys with Quantifiable Security against Invasive Readout", *IEEE/ACM International Conference On Computer Aided Design (ICCAD'17)*, pp 57-64, 2017. acceptance rate = 26% (105/399)

[15] **SN Dhanuskodi**, D Holcomb "An improved clocking methodology for energy efficient low area AES architectures using register renaming", *IEEE/ACM International Symposium on Low Power Electronics and Design (ISLPED'17)*, pp 1-6, 2017. acceptance rate = 25% (38/152)

[16] C. Yu, D.E. Holcomb, M. Ciesielski, "Reverse Engineering of Irreducible Polynomials in GF (2^m) Arithmetic", *Design Automation and Test in Europe (DATE)*, pp 1562-1567, Mar. 2017. acceptance rate = 24% (193/794)

[17] **S. Keshavarz**, C. Paar, D.E. Holcomb "Design Automation for Obfuscated Circuits with Multiple Viable Functions", *Design Automation and Test in Europe (DATE)*, pp 886-889, Mar. 2017.

[18] **S Keshavarz**, D Holcomb "Privacy Leakages in Approximate Adders", *IEEE International Symposium on Circuits and Systems (ISCAS)*, pp 1-4, May 2017.

[19] VC Patil, A. Vijayakumar, D Holcomb, S Kundu "Improving reliability of weak PUFs via circuit techniques to enhance mismatch", *IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pp 146-150, 2017.

[20] NK Dumpala, S. Patil, D. Holcomb, R. Tessier "Energy Efficient Loop Unrolling for Low-Cost FPGAs", *2017 IEEE 25th Annual International Symposium on Field-Programmable Custom Computing Machines (FCCM)*, pp 117-120, 2017.

[21] **S. N. Dhanuskodi**, D. Holcomb, "Energy Optimization of Unrolled Block Ciphers using Combinational Checkpointing", *RFIDSec 2016: 12th Workshop on RFID and IoT Security*, pp 47-61, 2016

[22] X. Xu, D.E. Holcomb, "Reliable PUF Design Using Failure Patterns from Time-Controlled Power Gating", *Defect and Fault Tolerance in VLSI and Nanotechnology Systems Symposium (DFT)*, pp 135-140, 2016

[23] **S. Vyas**, N.K. Dumpala, R. Tessier, D.E. Holcomb, "Improving the Efficiency of PUF-Based Key Generation in FPGAs using Variation-Aware Placement", *Field Programmable Logic (FPL)*, pp 1-4, 2016

[24] S. Ghandali, G.T. Becker, D. Holcomb, C. Paar "A Design Methodology for Stealthy Parametric Trojans and Its Application to Bug Attacks", *Cryptographic Hardware and Embedded Systems (CHES)*, pp 625-647, 2016 acceptance rate = 20% (30/148)

[25] **S. N. Dhanuskodi**, **S. Keshavarz**, D. Holcomb, "LLPA: Logic State Based Leakage Power Analysis", *International Symposium on VLSI (ISVLSI)*, pp 218-223, 2016

[26] X. Xu, W.P. Burleson D. Holcomb, "Using Statistical Models to Improve the Reliability of Delay-Based PUFs", *International Symposium on VLSI (ISVLSI)*, pp 547-552, 2016

[27] X. Xu, D. Holcomb, "A Clockless Sequential PUF with Autonomous Majority Voting", *Great Lakes Symposium on VLSI (GLSVLSI)*, pp 27-32, 2016 acceptance rate = 25% (50/197)

[28] **D. Liu**, C. Yu, **X. Zhang**, D.E. Holcomb "Oracle-Guided Incremental SAT Solving to Reverse Engineer Camouflaged Logic Circuits", *Design Automation and Test in Europe (DATE).*, pp 433-438, Mar. 2016. acceptance rate = 24% (199/829)

[29] A. Rahmati, M. Hicks, D. Holcomb, K. Fu, "Probable cause: the deanonymizing effects of approximate DRAM", *International Symposium on Computer Architecture (ISCA)*, pp 604-615, 2015 acceptance rate = 19% (58/309)

[30] X. Xu, U. Rührmair, D. Holcomb, W. Burleson "Security Evaluation and Enhancement of Bistable Ring PUFs", *Radio Frequency Identification: security and privacy issues (RFIDSec)*, pp 3-16, Jun. 2015

[31] D. Holcomb, K. Fu, "Building Native Challenge-Response PUF Capability into any SRAM", *Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, pp 510-526, Sep. 2014. acceptance rate = 26% (33/127)

[32] A. Rahmati, M. Hicks, D. Holcomb, and K. Fu, "Refreshing Thoughts on DRAM: Power Saving vs. Data Integrity", *Workshop on Approximate Computing Across the System Stack (WACAS)*, 2014

[33] D. Holcomb, K. Fu, "QBF-Based Synthesis of Optimal Word-Splitting in Approximate Multi-Level Storage Cells", *Workshop on Approximate Computing Across the System Stack (WACAS)*, 2014

[34] U. Rührmair, D. Holcomb, "PUFs at a glance", *Design Automation and Test in Europe (DATE)*, 2014 acceptance rate = 23% (206/890)

[35] S. Jha, M. Talalay, D. Holcomb, U. Ogras, M. Kishinevsky, M. Klinglesmith, R. De Gruijl and S. Choi, "Automated Design Space Exploration for SoC Interconnects", *Intel Design and Test Technology Conference (DTTC)*, 2013

[36] D. Holcomb, A. Rahmati, M. Salajegheh, W.P. Burleson, K. Fu, "DRV-Fingerprinting: Using Data Retention Voltage of SRAM Cells for Chip Identification", *Workshop on RFID Security and Privacy (RFIDSec)* Jul. 2012

[37] A. Rahmati, M. Salajegheh, D. Holcomb, J. Sorber, W.P. Burleson, K. Fu, "TARDIS: Time and Remanence Decay in SRAM to Implement Secure Protocols on Embedded Devices without Clocks", *USENIX Security Symposium*, Aug. 2012 acceptance rate = 19% (43/222)

[38] D. Holcomb, A. Gotmanov, M. Kishinevsky, S.A. Seshia, "Compositional Performance Verification of NoC Designs", *International Conference on Formal Methods and Models for Codesign (MEMOCODE)*, Jul. 2012

[39] D. Holcomb, B. A. Brady, S. A. Seshia, "Abstraction-Based Performance Analysis of NoCs", *Design Automation Conference (DAC)*, Jun. 2011 acceptance rate = 23% (156/690)

[40] B. A. Brady, D. E. Holcomb, S. A. Seshia, "Counterexample-guided SMT-driven optimal buffer sizing", *Design Automation and Test in Europe Conference (DATE)*, Mar. 2011

[41] L. Lin, D. Holcomb, D. K. Krishnappa, P. Shabadi, W. Burleson, "Low-Power Sub-threshold Design of Secure Physical Unclonable Functions", *International Symposium on Low Power Electronics and Design (ISLPED)*, Aug. 2010. acceptance rate = 24% (48/203)

[42] D. Holcomb, W. Li, S. A. Seshia, "Design as you see FIT: System-Level Soft Error Analysis of Sequential Circuits," *Design Automation and Test in Europe Conference (DATE)*, Apr. 2009 acceptance rate = 25% (226/895)

[43] V. Ambrose, W. Burleson, D. Holcomb, S. Mukherjee, J. Pickholtz, "A Fast and Accurate Method for Simulating Soft Errors in Large Combinatorial Logic Circuits", *Intel Design and Test Technology Conference (DTTC)*, 2007

[44] D.E. Holcomb, W.P. Burleson, and K. Fu, "Initial SRAM State as a Fingerprint and Source of True Random Numbers for RFID Tags," *Proceedings of the Conference on RFID Security (RFIDSec)*, Jul. 2007.

Selected Non Peer-Reviewed Publications and Talks

D. E. Holcomb, W. Li, S. A. Seshia, "Algorithms for Green Buildings: Learning-Based Techniques for Energy Prediction and Fault Diagnosis", *UC Berkeley Technical Report EECS-2009-138*, Oct. 2009

Voss, P.B., D.E. Holcomb, R.A. Zaveri, C.M. Berkowitz, "Integrated System Optimization of Controlled Meteorological (CMET) Balloons", *Proceedings of AIAA's 5th Annual Aviation Technology, Integration, and Operations (ATIO) Conference and AIAA 16th Lighter-than-air systems technology conference and balloons systems conference*, Sept. 2005.

Invited Talks and External Seminars:

- "Counterfoil: Verifying provenance of integrated circuit packages" *Embedded Sec. Workshop,* Aug. 2020
- "Hardware Security in multi-tenant FPGAs"
  - *UC Berkeley,* Nov. 2019
  - *WPI,* Sept 2019
- "Secure Dust - a compact AES implementation in 16nm technology for sub-pJ per bit encryption"
  - *Intel Circuit Research Lab*, Hillsboro OR, August 6, 2019
  - *SRC e-Workshop*, July 19, 2019
- "Hardware Security in multi-tenant FPGAs" *Intel SCAP* June 2019
- "Obfuscation and Reverse Engineering of Keys and IP,"
  - *UConn,* Feb 23, 2017
  - *Ruhr University Bochum,* Germany, July 6, 2017
- "Protecting keys and IP against invasive readout," *MIT Lincoln Lab.,* Lexington MA, May 22, 2017
- "SRAM-based Physical Unclonable Functions,"
  - *MITRE,* Bedford MA, Nov. 20, 2015
  - *WPI,* Feb. 26, 2015
- "Formal Performance Verification of NoCs," *Gigascale Systems Research Center,* Sept. 18, 2012
- "FERNS: Fingerprint Extraction and Random Numbers from SRAM," *TSMC,* San Jose, May 25, 2010

Awards

- 2020 UMass ECE department dissertation prize won by my student Siva Nishok Dhanuskodi
- 2019 FPL Conference "Stamatis Vassiliadis" Best Paper award (lead author G. Provelengios)
- 2019 ISVLSI Conference Best Poster award (lead author S. N. Dhanuskodi)
- 2018 HOST Conference Best Poster award (lead author S. Keshavarz)
- 2018 NSF CAREER award
- 2016 ECE Faculty Best Hair award (as voted by IEEE Student Branch)
- Intel Division Recognition Award for Soft Error Estimation Tool

Patents

Denis Foo Kune, Benjamin Andrew Ransford, Daniel Edward Holcomb, Andrew Whitehouse DeOrio "Anomaly and malware detection using side channel analysis" U.S. Patent 11,201,885 14 Dec 2021 (Virta Laboratories)

Denis Foo Kune, Benjamin Andrew Ransford, Daniel Edward Holcomb "Anomaly and malware detection using side channel analysis" U.S. Patent 10,693,896 23 June 2020 (Virta Laboratories)

D.E. Holcomb, K. Fu. "Physical unclonable function using augmented memory for challenge-response hashing" U.S. Patent 10,038,564. 31 July 2018

D.E. Holcomb, K. Fu. "Physical unclonable function using augmented memory for challenge-response hashing" U.S. Patent 9,787,481. 10 October 2017

W.P. Burleson, S.S. Mukherjee, V. Ambrose, D.E. Holcomb. "Generalized Interlocked Register Cell." U.S. Patent 7,529,118. 5 May 2009. (Intel)

Service

Sessions and events chaired or organized:

- Organized New England Hardware Security Day at UMass
  Jointly with Yale, WPI, Northeastern (`http://vernam.wpi.edu/nehws22/`)
  Marriott Center, 4/1/2022, over 100 attendees, NSF supported
- Program co-chair at ASHES 2018 and ASHES 2019
- Session chair/co-chair at DAC 2016, 2018, 2019, CHES 2020, DATE 2021
- Finance and Publication chair, ARITH 2018
- Registration chair, ICCD 2020
- Co-organized Hack@DAC: The DAC Hardware Security Contest in 2017/2018/2019/2020
  (`https://hack-dac19.trust-sysec.com/`)
- Co-organized NSF Workshop on Foundations of Secure and Trusted Hardware (FOSTER) 2017
  (`https://wp.nyu.edu/foster/`)
- Co-organizer of New England Security Day in Sept 2015

Member of technical program committees:

- Network and Distributed System Security Symposium (NDSS) 2022, 2023
- ACM Conference on Computer and Communications Security (CCS) 2021, 2022
- Cryptographic Hardware and Embedded Systems (CHES) 2016, 2019, 2020
- Design Automation Conference (DAC) 2016, 2017, 2018
- Malicious Software and Hardware in Internet of Things (Mal-IoT) 2018, 2019
- Workshop on Attacks and Solutions in Hardware Security (ASHES) 2017, 2018, 2019
- Workshop on Hardware and Architectural Support for Security and Privacy (HASP) 2018, 2019, 2020
- Workshop on Top Picks in Hardware and Embedded Security 2018, 2019, 2020
- IEEE Conference on Communications and Network Security (CNS) 2016
- Workshop on RFID Security and Privacy (RFIDSec) 2015, 2016
- International Workshop on Trustworthy Embedded Devices (TrustED) 2015
- Secure Component and System Identification (SECSI) 2010

Guest editor for journals:

- IEEE Design & Test of Computers, special issue on Hack@DAC
- Journal of Cryptographic Engineering, special issue for ASHES 2019

Reviewer for journals including the following:

- IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems
- IEEE Transactions on VLSI Systems
- IEEE Transactions on Computers
- IEEE Transactions on Circuits and Systems
- IEEE Transactions on Dependable and Secure Computing (TDSC)
- IEEE Transactions on Information Forensics & Security (TIFS)
- IEEE Computer Architecture Letters
- Nature Electronics

Grant review:

- NSF on-site panel (2016, 2017, 2018, 2019), remote panel (2019, 2020, 2022)

- NSF ad-hoc reviewer (2014, 2019)
- Agence Nationale De La Recherche (France) external review (2020)
- Israel Science Foundation, external review (2020)
- DFG - Deutsche Forschungsgemeinschaft (Germany) external review (2022)

University and College Service:

- Director of Transfer Affairs, ECE Department (2017-2021)
- New/transfer Student Orientation (2015,2016,2017,2018,2019,2020,2021)
- ECE Department Seminar Committee (2015,2016,2018)
- ECE Department Personnel Committee (2017,2021)
- Member of hiring committees (2x 2016-7)
- Tau Beta Pi faculty adviser (2017-2020)

Grants Awarded

[1] "Hardware Security for Machine Learning and Supply Chain"
Raytheon Corporation
D.E. Holcomb (PI), W. Burleson (Co-PI), R. Tessier (Co-PI), A. Houmansadr (Co-PI)
10/1/2021 - 12/31/2021 ; $75,000

[2] "Chiplet PUFs for hardware security"
MITRE Corporation
W. Burleson (PI), D.E. Holcomb (Co-PI)
7/1/2021 - 7/1/22 ; $339,959

[3] " FMitF: Track I: Privacy-Preserving Policy Verification of Interdomain Routing"
National Science Foundation
L. Gao (PI), D.E. Holcomb (Co-PI)
10/1/2019 - 9/30/2023 ; $749,998

[4] " SaTC: CORE: Medium: Collaborative: Security of Reconfigurable Cloud Computing"
National Science Foundation
R. Tessier (PI), D.E. Holcomb (Co-PI)
7/1/2019 - 6/30/2023 ; $690,839

[5] "CAREER: Supply Chain Security for Integrated Circuits"
National Science Foundation
D. E. Holcomb (PI)
2/1/2018 - 1/31/2023 ; $596,160

[6] "True Random Number Generation on Amazon EC2 F1"
Gradient Technologies
R. Tessier (PI), D.E. Holcomb (Co-PI)
11/2/2017 - ; $20,000

[7] "Security for multi-Tenant FPGAs"
Intel Corporation
R. Tessier (PI), D.E. Holcomb (Co-PI)
11/2/2017 - ; $365,000

[8] "Defending against against Advanced Physical Attacks"
Raytheon
W. Burleson (PI), D.E. Holcomb (Co-PI)
9/1/2017 - ; $50,000

[9] "Designing Strongly Obfuscated Hardware with Quantifiable Security against Reverse Engineering"
National Science Foundation
C. Paar (PI), D.E. Holcomb (Co-PI), S. Kundu (Former Co-PI)
8/1/2016 - 7/31/2020; $1,163,227
6/1/2018 - 8/31/2018; $7,500 REU supplement

[10] "SecureDust – The Physical Limits of Information Security"
National Science Foundation and Semiconductor Research Corporation
D.E. Holcomb (PI), W.P. Burleson (Co-PI), R. Tessier (Co-PI)
9/1/2016 - 8/31/2019; $462,212

[11] "Investigating Stealthy Hardware Trojans"
National Science Foundation
C. Paar (PI), D.E. Holcomb (Co-PI), S. Kundu (Former Co-PI)
9/1/2014 - 8/31/2018; $499,997

[12] "CyberCorps Scholarship for Service at the University of Massachusetts Amherst"
National Science Foundation
B. Levine (PI), W.P. Burleson (Co-PI), M. Liberatore (Co-PI), D.E. Holcomb (Co-PI)
9/1/2021 - 8/31/2026; $4,424,837

[13] "CyberCorps Scholarship for Service at the University of Massachusetts Amherst"
National Science Foundation
B. Levine (PI), W.P. Burleson (Co-PI), M. Liberatore (Co-PI), M. Getmansky Sherman (Co-PI), E. Sommers (Co-PI), E. Berger (Senior Personnel), Y. Brun (SP), L. Clarke (SP), D.E. Holcomb (SP), A. Houmansadr (SP), L. Gao (SP), K. Gile (SP), A. Guha (SP), G. Miklau (SP), A. Nagurney (SP), R. Wright (SP)
9/1/2016 - 8/31/2021; $4,159,336

Research Advising

Theses In Progress, with Anticipated Role of Chair or Co-chair

- Xiang Li (PhD; post-proposal)
- Bharadwaj Madabhushi (PhD)
- Thiago Costa de Paiva (PhD; co-advise with Physics Dept)
- Aleksa Deric (PhD)
- Arjun Suresh (PhD)
- Shahriar Hadayeghparast (PhD)

- Peter Stanwicks (MS)
- Mohammad Waquas Usmani (MS)

Theses Completed, with Role of Chair or Co-chair

- Shahrzad Keshavarz (PhD, Dec. 2019; first employment Cadence Design Systems)
- Siva Nishok Dhanuskodi (PhD, Dec. 2019; first employment UMass ECE PostDoc)

- Chethan Ramesh (MS, Aug. 2019; co-chair with Russell Tessier; first employment Apple)
- Harshavardhan Ramanna (MS, May 2019; first employment Qualcomm)
- Neev Kiran (MS, Aug. 2018; co-chair with Sunghoon Ivan Lee; continuing in UMass CS PhD program)
- Mohammad Aftab Usmani (MS, Oct. 2017; first employment Netronome)
- Xiangyu Zhang (MS, May 2017; first employment Intel)
- Shrikant Vyas (MS, Sept. 2016; co-chair with Russell Tessier; first employment Altera)

- Richard Hartnett (BS Honors, May 2018; First employment Palo Alto Networks)
- Thomas Baim (BS Honors, May 2018; First employment BAE)
- Omid Meh (BS Honors, May 2016; First employment IBM)

Theses Completed, with Role of Committee Member

- George Provelengios (PhD)
- Md Nazmul Islam (PhD)
- Arunkumar Vijayakumar (PhD)
- Xiaolin Xu (PhD)
- Meng-Chieh (Joe) Chiu (PhD - CS)
- Mingyu Li (PhD)
- Jiajun Shi (PhD)
- Cunxi Yu (PhD)
- Samaneh Ghandali (PhD)
- Vinay Patil (PhD)
- Tiankai Su (PhD)
- Falk Schellenberg (PhD, RU Bochum; role of secondary referee)
- Wenjie Xiong (PhD, Yale; role of external reader)
- Atif Yasin (PhD)
- Xiaozhe Shao (PhD)

- Zibin Chen (MS)
- Mythili Vishalini Anbazhagan (MS)
- Shivukumar Patil (MS)
- Yunning Li (MS)
- Sourabh Kulkarni (MS)
- Sachin Bhat (MS)
- Xue Ouyang (MS)
- Vijaya Deepak Kadirvel (MS)
- Naveen Kumar Dumpala (MS)
- Jackie Lagasse (MS)

- Ethan Miller (BS)
- Cyril Caparanga (BS)
- Walter Brown (BS)
- Andrew Hartnett (BS)
- Shaun Ghosh (BS)
- Joseph Maloyan (BS)

NSF REUs Advised

- Samuel Allen (2019)
- Peter Stanwicks (2018)