# Daniel Holcomb

CONTACT INFORMATION

309H 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, Cyber-Physical Systems, On-chip Networks, Approximate Computing

## 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

*Assistant Professor* **Jan 2015 - Present**
Tenure track faculty focusing on embedded systems and security, EDA, and health monitoring

**University of Michigan**, Ann Arbor, MI USA

*Research Fellow* **Oct 2013 - Dec 2014**
Research on medical security, embedded systems security, and approximate computing

**UC Berkeley**, Berkeley, CA USA

*Graduate Student Researcher* **Spring 2007 - Summer 2013**
Applied formal methods to variety of problems, culminating in dissertation on NoC QoS verification

**UMass Amherst**, Amherst, MA USA

*Graduate Research Assistant, ECE* **Fall 2005 - Summer 2007**
Worked on combinational logic soft errors, process variation and embedded security. Invented techniques for IC Fingerprinting and Random Number Generation from SRAM power-up state

*Undergraduate Research Assistant, Atmospheric Research Lab* **Summer 2004 - Summer 2005**
Responsible for research payload of world's smallest altitude controlled balloons. Deployed payloads during major air-quality studies, in NH (ICARTT-2004) and TX (SETTS).

**Smith College**, Northampton, MA USA

*Consultant, Atmospheric Research Lab* **Fall 2005**
Contributed to further development of atmospheric research payload that was undergraduate thesis project

## INDUSTRY APPOINTMENTS

**Virta Labs**, Ann Arbor, MI USA

*Hardware Engineering Lead* **Jan 2014 - Present**
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 verification
- Achieved 100x speedup in formal verification of latency bounds on ring interconnects
- Implemented heuristic optimization for SoC design space exploration

**Intel**, Hudson, MA USA

*Graduate Technical Intern* **Spring-Summer 2006; Summer 2007**
Worked on analysis and mitigation of particle-strike induced errors in combinational circuits and memories
- Created tool to find soft-error contribution of each gate in multi-thousand gate combinational circuits
- Received division recognition award, awarded U.S. Patent for soft-error resistant register

---

## Teaching

**UMass Amherst**, Amherst, MA USA

*ECE697MB: Modeling and Verification of Embedded Systems* **Spring 2015, Spring 2016, Spring 2017**
Graduate and undergraduate course on reasoning about embedded systems
- Using Lee and Seshia textbook, with research papers
- Topics covered include discrete and hybrid reachability, scheduling, etc

*ECE591CF: Cybersecurity Faculty Lecture Series* **Fall 2015, Fall 2016**
Co-organized 1-credit seminar course of rotating speakers from various department at UMass

*ECE353: Computer Systems Lab* **Fall 2015, Fall 2016, Fall 2017**
Undergraduate course on applied embedded systems course
- Verilog programming for CPLD-based system
- C programming of ATmega32 processor

*ECE296/ECE396: Embedded Capture The Flag Competition (Independent Study)* **Spring 2016, Spring 2017**
Organized and supervised a team of undergraduate CS and ECE students competing against other Universities in MITRE-sponsored hacking contest (18 total students participated).

*ECE696: Independent Study*
Supervised graduate student independent study projects
- Abhinav Khandelwal: "Design Space Exploration of Error Correction Techniques for Physical Unclonable Functions," Fall 2015
- Mohammad Aftab Usmani: "Evaluation of the feasibility of implementing Anderson PUF using SLICE-L cells on Virtex 7 FPGA," Spring 2016

*ECE499: Capstone Honors Project*
Supervised year-long capstone project of Commomwealth College students
- Omid Meh (2016): "Automated Mussel Detection Using Mobile Phone Microscopy and Microfluidic Techniques"

*Senior Design Project* **2015, 2016, 2017**
Supervised undegraduate teams on their year-long design project

---

## Peer-Reviewed Publications

### 2017

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.

S Keshavarz, D Holcomb "Threshold-based Obfuscated Keys with Quantifiable Security against Invasive Readout", *IEEE/ACM International Conference On Computer Aided Design (ICCAD'17)*, 2017.

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

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)*, 2017.

C. Yu, X. Zhang, D. Liu, M. Ciesielski, D. Holcomb, “Incremental SAT-based Reverse Engineering of Camouaged Logic Circuits”, *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 2017

C. Yu, D.E. Holcomb, M. Ciesielski, “Reverse Engineering of Irreducible Polynomials in GF ($2^m$) Arithmetic”, *Design Automation and Test in Europe (DATE)*, Mar. 2017.

S. Keshavarz, C. Paar, D.E. Holcomb “Design Automation for Obfuscated Circuits with Multiple Viable Functions”, *Design Automation and Test in Europe (DATE)*, Mar. 2017.

S Keshavarz, D Holcomb “Privacy Leakages in Approximate Adders”, *IEEE International Symposium on Circuits and Systems (ISCAS)*, 2017.

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)*, 2017.

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)*, 2017.

## 2016

S. N. Dhanuskodi, D. Holcomb, “Energy Optimization of Unrolled Block Ciphers using Combinational Checkpointing”, *RFIDSec 2016: 12th Workshop on RFID and IoT Security*, 2016

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)*, 2016

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)*, 2016

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)*, 2016

S. Ghandali, G.T. Becker, D. Holcomb, and C. Paar “A Design Methodology for Stealthy Parametric Trojans and Its Application to Bug Attacks”, *Cryptographic Hardware and Embedded Systems (CHES)*, 2016

S. N. Dhanuskodi, S. Keshavarz, and D. Holcomb, “LLPA: Logic State Based Leakage Power Analysis”, *International Symposium on VLSI (ISVLSI)*, 2016

X. Xu, W.P. Burleson D. Holcomb, “Using Statistical Models to Improve the Reliability of Delay-Based PUFs”, *International Symposium on VLSI (ISVLSI)*, 2016

X. Xu, D. Holcomb, “A Clockless Sequential PUF with Autonomous Majority Voting”, *Great Lakes Symposium on VLSI (GLSVLSI)*, 2016

J. Hester, N. Tobias, A. Rahmati, L. Sitanayah, D. Holcomb, K. Fu, W.P. Burleson, and J. Sorber. “Persistent Clocks for Batteryless Sensing Devices”, *ACM Trans. Embed. Comput. Syst. 15, 4, Article 77* August 2016

D. Liu, C. Yu, X. Zhang, and D.E. Holcomb “Oracle-Guided Incremental SAT Solving to Reverse Engineer Camouflaged Logic Circuits”, *Design Automation and Test in Europe (DATE).*, Mar. 2016.

## 2015

A. Rahmati, M. Hicks, D. Holcomb, K. Fu, "Probable cause: the deanonymizing effects of approximate DRAM", *International Symposium on Computer Architecture (ISCA)*, 2015

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*, Jun. 2015

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

## 2014

D. Holcomb, K. Fu, "Building Native Challenge-Response PUF Capability into any SRAM", *Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, Sep. 2014

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

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

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

U. Rühmair, D. Holcomb, "PUFs at a glance", *Design Automation and Test in Europe (DATE)*, 2014

## 2013

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

## 2012

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

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

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

## 2011

D. Holcomb, B. A. Brady, S. A. Seshia, "Abstraction-Based Performance Analysis of NoCs", *Design Automation Conference (DAC)*, Jun. 2011

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

## 2010

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.

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.

## 2009

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*, Sept. 2009.

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

## 2007

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

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.

## 2006

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.

---

## 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:
- “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
- “SRAM-based Physical Unclonable Functions,” *WPI,* Feb. 26, 2015
- “SRAM-based Physical Unclonable Functions,” *MITRE,* Bedford MA, Nov. 20, 2015
- “Protecting keys and IP against invasive readout,” *MIT Lincoln Laboratory,* Lexington MA, May 22, 2017

## Selected Press Coverage

Anderson, Mark. "Could an SRAM Hourglass Save RFID Chips Just in Time?" *IEEE Spectrum.*, Aug. 6, 2012. `http://spectrum.ieee.org/semiconductors/memory/could-an-sram-hourglass-save-rfid-chips-just-in-time`

"Time Machines, Computer Memory, and Brute Force Attacks Against Smartcards." *Slashdot.*, Aug. 6, 2012. `http://it.slashdot.org/story/12/08/07/006229`

Anderson, Mark. "Quirks of RFID Memory Make for Cheap Security Scheme." *IEEE Spectrum.*, Mar. 18, 2009. `http://spectrum.ieee.org/computing/hardware/quirks-of-rfid-memory-make-for-cheap-security-scheme`

O'Connor, Mary Catherine. "UMass Researchers Describe New Approach to Tag Security." *RFID Journal.* Nov. 1, 2007. `http://www.rfidjournal.com/articles/view?3723`

Jackson, Joab. "Secure RFID tags?" *Government Computer News.* Sept. 24, 2007. `http://gcn.com/articles/2007/09/24/secure-rfid-tags.aspx`

"Ultra-low-cost True Randomness." *Slashdot.*, Sept. 10, 2007. `http://it.slashdot.org/story/07/09/10/147238`

Jackson, Joab. "NSF researchers produce RFID random number generator." *Government Computer News.* Sept. 12, 2007. `http://gcn.com/articles/2007/09/12/nsf-researchers-produce-rfid-random-number-generator.aspx`

## Patents

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

K.E. Fu, D.E. Holcomb, W.P. Burleson. "Methods and Systems for Characterizing and Identifying Electronic Devices." U.S. Patent Pending, Application Serial No. 13/930,855. 28 June 2013. (UMass)

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

Grant review:
- NSF 2017 on-site panel
- NSF 2016 on-site panel
- NSF 2014 ad-hoc

Sessions and events chaired or organized:
- Co-chair embedded systems security session at DAC 2016
- Co-organized VLSI security special session at DFT 2016
- Co-organized Hack@DAC: The DAC 2017 Hardware Security Contest (`https://wp.nyu.edu/hackdac17/`)
- Co-organized Hack@DAC: The DAC 2018 Hardware Security Contest (`https://hack-dac18.trust-sysec.com/`)
- Co-organized NSF Workshop on Foundations of Secure and Trusted Hardware (FOSTER) 2017 (`https://wp.nyu.edu/foster/`)

Member of technical program committees:
- Design Automation Conference (DAC) 2016, 2017, 2018
- Malicious Software and Hardware in Internet of Things (Mal-IoT) 2018
- Workshop on Attacks and Solutions in Hardware Security (ASHES) 2017
- Cryptographic Hardware and Embedded Systems (CHES) 2016
- 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

Active reviewer for top-tier conferences and journals in embedded systems, security, VLSI, and formal methods, including the following venues:

- ACM Conference on Computer and Communications Security (CCS)
- 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/ACM International Conference on Computer-Aided Design (ICCAD)
- IEEE International Symposium on Circuits and Systems (ISCAS)
- International Conference on Computer Aided Verification (CAV)
- International Conference on Embedded Software (EMSOFT)
- International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS)
- Formal Methods in Computer-Aided Design (FMCAD)

Co-organizer of New England Security Day in Sept 2015 with over 100 attendees.

Adviser to students in NSF-funded Scholarship For Service program

University and College Service:
- Director of Transfer Affairs, ECE Department (2017-)
- New Student Orientation (2015,2016,2017)
- ECE Department Seminar Committee (2015,2016)

---

## Grants Awarded

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

"Security for multi-Tenant FPGAs" Intel Corporation
R. Tessier (PI), D.E. Holcomb (Co-PI)
11/2/2017 - ; $90,000

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

TWC:Medium "Designing Strongly Obfuscated Hardware with Quantifiable Security against Reverse Engineering"
National Science Foundation
C. Paar (PI), D.E. Holcomb (Co-PI), S. Kundu (Co-PI)
8/1/2016 - 7/31/2020; $1,163,227

STARSS:Small "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

TWC: TTP Option: Small: "Investigating Stealthy Hardware Trojans"
National Science Foundation
C. Paar (PI), S. Kundu (Former Co-PI), D.E. Holcomb (Co-PI)
9/1/2014 - 8/31/2017; $499,997

"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

---

## Theses Advised

I have been the primary thesis adviser or co-primary thesis adviser for the following students:

- Siva Nishok Dhanuskodi (PhD, in progress)
- Shahrzad Keshavarz (PhD, in progress)
- Xiangyu Zhang (MS, defended May 2017)
- Mohammad Aftab Usmani (MS, defended October 2017)
- Shrikant Vyas (MS, Sept. 2016; co-advised with Russell Tessier)
- Harshavardhan Ramanna (MS, in progress)
- Omid Meh (BS Honors)
- Richard Hartnett (BS Honors, in progress)
- Thomas Baim (BS Honors, in progress)

I have been on the thesis committee of the following students:
- Arunkumar Vijayakumar (PhD)
- Xiaolin Xu (PhD)
- Meng-Chieh Chiu (PhD - CS)
- Mingyu Li (PhD)
- Jiajun Shi (PhD)
- Sourabh Kulkarni (MS)
- Sachin Bhat (MS)
- Xue Ouyang (MS)
- Vijaya Deepak Kadirvel (MS)
- Walter Brown (BS)