Center for Embedded Systems for Critical Applications

VirginiaTech
Invent the Future

CESCA Newsletter

Center for Embedded Systems for Critical Applications

CESCA • 302 Whittemore Hall • Dept. of ECE • Virginia Tech • Blacksburg • 24061 • USA

October 2012· No.008

The **Center for Embedded Systems for Critical Applications** is a research center within the Bradley Department of Electrical and Computer Engineering. CESCA addresses the major challenges in the conception, the design, and the implementation of next-generation embedded systems. CESCA bundles the efforts of seven faculty and their students in a cross-disciplinary setting. CESCA generates know-how, expert advice, and skilled researchers who tackle the needs of tomorrow's industry and academia.

CESCA's Industry Affiliate Program

The projects carried out by CESCA Faculty and their students represent a valuable resource of intellectual property. CESCA has a model in place that helps industry to benefit from this know-how and these results - CESCA's Industry Affiliate Program (IAP).

The objective of CESCA's IAP is to provide industrial partners with privileged access to our results including graduating students, faculty know-how, and project intellectual-property. We offer three specific benefits for IAP members. First, an IAP member may engage CESCA in directed research, by initiating collaboration around a specific research problem. Second, an IAP member may team up with CESCA Faculty to write proposals for government funding (such as SBIR). Third, an IAP member may engage CESCA Faculty in one-on-one consulting, providing external expert advice on specific research problems. In addition to the above mentioned benefits, IAP members of CESCA also get early access to CESCA's major product - graduating students. Our graduating students are experts in the research topic of their advisor. By working with CESCA Faculty through the IAP program, affiliates will get in touch with students early-on. In return for these benefits, CESCA affiliate members contribute a yearly membership fee. There are two levels of membership. The basic IAP costs $10K per year, and includes the above benefits apart from directed research. The extended IAP costs $40K per year, and includes support of a graduate student specifically assigned to support the affiliate member in directed research.

Full details of the CESCA Affiliate Program may be found at the CESCA website, through the URL http://www.cesca.centers.vt.edu/Affiliate/index.html. Questions and requests for further information may be directed to Patrick Schaumont (schaum@vt.edu).

CESCA Alumnus Establishes a New Startup

Michael Henry graduated in Dec. 2011 with a Ph.D in Computer Engineering (advisor: Leyla Nazhandali) and started an engineering R&D company. He currently has Phase 1 SBIR funding from the Air Force to design and eventually prototype a low-power military-capable GPS receiver. This project involves collaboration with the VLSI Design/Automation lab at the University of Michigan, Ann Arbor and he is currently based in Ann Arbor. In addition to working towards Phase 2 funding on the Air Force contract, he is also applying for other SBIR contracts relating to advanced wide-spectrum CMOS image sensors and neuromorphic image processing.

From the Director's Desk

At the start of the academic 2012-2013 year, CESCA is more than ever the place to be in embedded systems design for critical applications. Let me explain.CESCA's objective is to become a one-stop shop for expertise and know-how in embedded systems design. We do this as follows. We start by hand-picking the brightest students, and by transforming them, through research projects, into domain experts. Along the way, we demonstrate proof-of-concept designs and we publish our findings.

But then comes the essential ingredient. The seven faculty in CESCA engage in cross-disciplinary research to tackle design problems that cannot be addressed by stand-alone design teams. For example, we develop advanced fingerprint matching techniques by considering methods from digital system verification. We develop novel sensor node architectures that have a fully flexible yet high-performance architecture. We improve software radio security by building better, trustworthy hardware architectures for them. CESCA faculty combines the expertise at all these abstraction levels, and they collaborate to devise entirely new solutions to hard and unsolved problems.

The graduating students are CESCA's key product. They embody the know-how of their research advisor, the expertise of their research project, and the spirit of CESCA collaboration. In the past 4 years, CESCA graduated an average of 6 PhD level students per year. This semester, we welcome four new PhD students and one MS, and they join a research group of 28 PhD and 5 MS students.

In this newsletter, you'll find an overview of the recent projects and achievements of CESCA faculty and their students. We address this newsletter especially to our embedded-industry partners. One of the leading articles explains our Industry Affiliate Program, and the articles in this newsletter demonstrate CESCA expertise in critical embedded system design.

This new semester is a period of exciting changes in CESCA. Multiple new projects, some of them announced in this newsletter, are about to start. Several faculty have moved labs to foster close collaboration. We have hired a web developer to ensure we serve our students and project partners well.

Without doubt the biggest change is that Prof. Ha and Prof. Shukla, both CESCA founders, have moved on to new challenges. Prof. Ha became director of the newly founded Center for Multifunctional Integrated Circuits and Systems (MICS). Prof. Shukla joined the Hume center in VTRC Arlington.

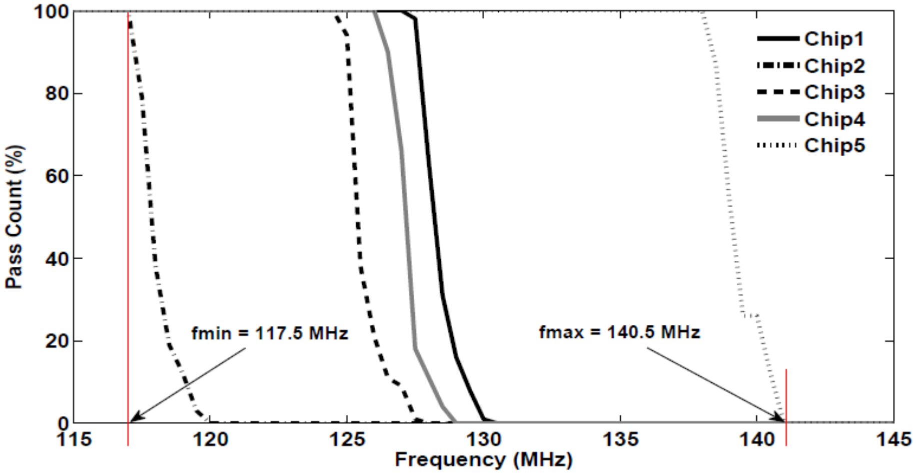
Over the past 9 years, both of them have set an example of vision and leadership for CESCA. Dr. Ha and Dr. Shukla, we will be indebted for many years to come. Now it's up to all of CESCA, faculty and students, to carry it on. And they will, because they can. CESCA faculty and students like the challenges, the collegiality, the spirit of research, and the rush of achievement.
I wish everyone a successful semester!

Patrick Schaumont
CESCA Director

News Items

Novel Microprocessor-based Physical Unclonable Function Demonstrated

The Secure Embedded Systems (SES) lab in CESCA has demonstrated a novel Physical Unclonable Function (PUF), implemented in a microprocessor. An on-chip PUF is an integrated structure that creates a chip-unique response. It can be used to uniquely distinguish one single chip among a large population of identical chips. PUFs are used for cryptographic key generation, and for authentication. Most of the existing PUF designs, however, consume a high amount of silicon resources and/or energy. This makes them less useful for embedded implementations.



Characterization of an ADD instruction for identical processors implemented in 5 different FPGA chips.

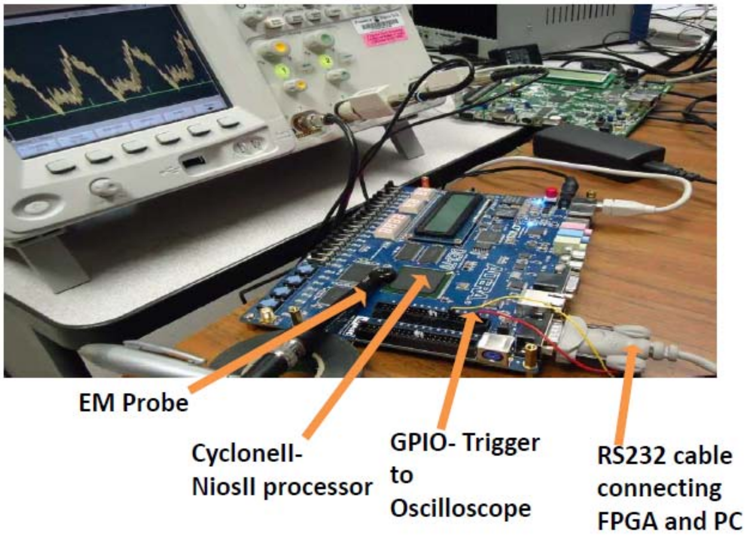
Using overclocking techniques, Abhranil Maiti (PhD student at SES), was able to demonstrate the uniqueness of a single microprocessor chip by observing its failure points due to the overclocking. The advantage of the technique, which is non-destructive, is that it is driven using software, and that it makes use of an existing microprocessor. The technique was demonstrated on a LEON-3 processor configured in Xilinx Spartan FPGA, but it is generally applicable to other microprocessors for which clock scaling is available. The novel PUF will be presented at the 2012 International Conference on Field Programmable Logic and Applications.

Undergraduate Researchers demonstrate Secure Measurement Toolkit

This summer, a team of undergraduate and graduate researchers of the Secure Embedded Systems Lab at Virginia Tech has built a prototype measurement toolkit for side-channel analysis. The toolkit, called SCAMeter, can be used to quickly analyze an embedded system design for side-channel leakage. It is an important component to support research in side-channel analysis countermeasures, one of the main efforts of the Secure Embedded Systems Lab.

A side-channel analysis infrastructure is a complex piece of software, which combines control software, data-aqcuisition software, embedded interfacing, and data storage and manipulation. Integrating various software components in a single consistent Python API, the team including

Cegil Kendir and Michael Cantrell was able to provide a scripted solution to side-channel analysis. The toolkit supports a designer in quickly integrating a device under test in a test harness, applying suitable stimuli, collecting side-channel measurements, and organizing the resulting measurements in an online database. SCAMeter will be used in the ongoing research projects of Schaumont in side-channel countermeasure design.



Components of a side-channel analysis setup include an oscilloscope, and embedded board, and a control PC.

CESCA Seminar Series and Video Channel

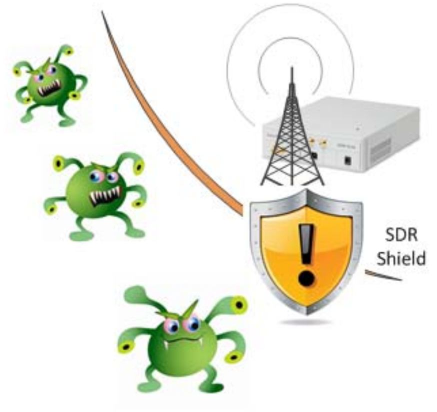
CESCA continues to hold regular research seminars, and to make most of them available on the CESCA video channel https://vimeo.com/cescavirginiatech. In Fall of 2012, Dr. Yaling Yang is organizing the series. The following is the schedule of upcoming talks.

9/7/2012:	Jonathan Graf (Directory SCC, Luna Innovations): FGPA Trust - Ensuring Design Integrity through Analysis of FPGA Bitstreams and IP Cores
9/14/2012:	Carlos Aguayo Gonzalez (CRO, Power Fingerprinting, Inc): Power Fingerprinting for integrity assessment of critical embedded systems
9/21/2012:	Amira Youssef (Information Technology Institute at Alexandria, Egypt) Image Watermarking Techniques Using Histogram Tailored Chaotic Maps
9/28/2012:	Wu Feng (Virginia Tech) An Ecosystem for the New HPC: Heterogeneous Parallel Computing
10/5/2012:	Nathan Li (Batelle Memorial Institute) The Chronicles of Cyber Security: The offense, the defense and the analytics
10/19/2012:	Linda Xie (Univ. of North Carolina--Charlotte)
11/30/2012:	Xiaokang Qiu (University of Illinois at Urbana Champaign)
12/7/2012:	Pamela Abhisre (University of Maryland)

CESCA gratefully acknowledges the students of its Seminar Recording Group, who produce video recordings of all major CESCA events. Members of this group are Avinash Desai and Mahesh Nanjundappa.

New Research Projects

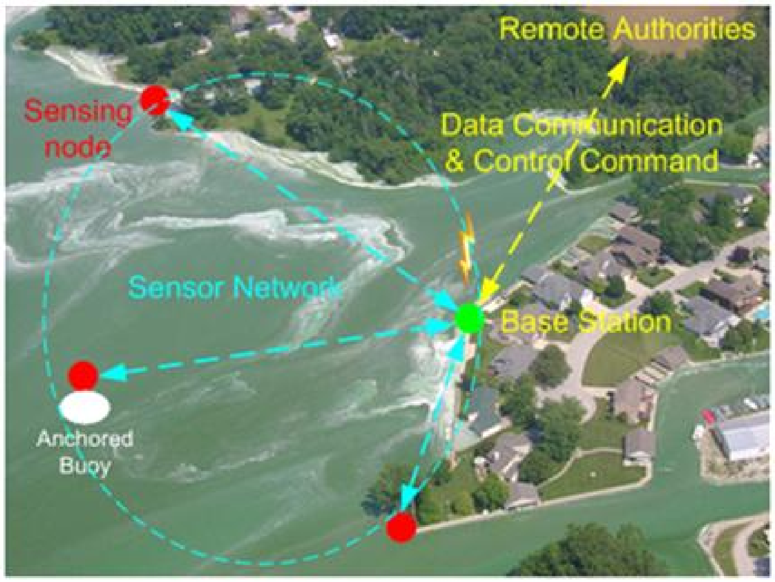
SDR Shield: A Hardware-based Security Solution for Software Defined Radio



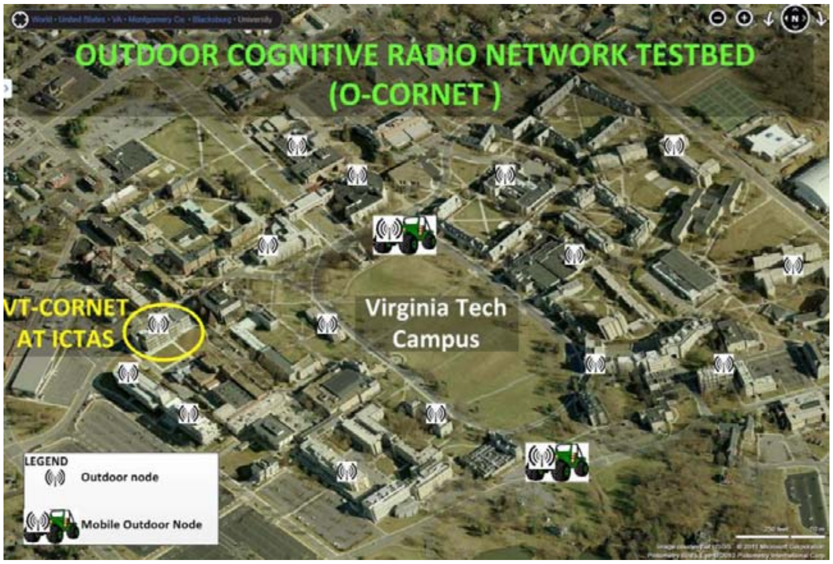
CESCA members Dr. Yaling Yang and Chao Wang with Co-PI Jeff Reed have recently won a $700,000 multiyear National Science Foundation (NSF) award. The project, titled “SDR Shield: A Hardware-based Security Solution for Software Defined Radio”, aims at designing an effective hardware-based SDR integrity assessment and behavior regulation device named SDR Shield.

Software Defined Radio (SDR) technology has the flexibility of implementing a large part of radio’s physical layer functions in software. It is one of the major technologies that will provide broadband services to millions of US residences. However, unlike conventional radio whose RF signals are tightly regulated by FCC-certified hardware, the software components of SDR can be easily exploited by hackers to create a wide range of unauthorized waveforms to launch attacks on many security-critical wireless systems. The existing preventive software-based security counter measures are not possible to prevent the myriad of potential software security loopholes and themselves often become targets of the malware. The limitations of existing works regarding SDR security lead to the proposed development of SDR Shield. SDR Shield resides between the vulnerable SDR software and the security-critical SDR hardware to detect any malicious configuration of the RF device and prevent it from being used to attack wireless systems. The SDR Shield uses side channel and communication channel information from different SDR components to detect deviations from expected execution status. SDR shield also includes a regulation circuit to enforce safety-critical properties of SDR operation. A secure update process is developed to maintain SDR shield’s flexibility and its own security. The generality of SDR Shield’s design provides a unified security mechanism for SDR design and hence can ease the burden on FCC or any future SDR design verification institutes in certifying security measures of SDR products.

In Situ Sensing System for the Selective and Sensitive Detection of Biological Toxins in Harmful Algal Blooms



Dr. Jerry Park working together with researchers from Univ. of Texas at Arlington recently started a project entitled “In Situ Sensing System for the Selective and Sensitive Detection of Biological Toxins in Harmful Algal Blooms”. This project is sponsored by the National Institute of Environmental Health Sciences (NIEHS), which is a part of the National Institute of Health (NIH), through a grant totaling $585K. The increasing occurrence of harmful algal blooms (HABs) in water resources worldwide is alarming the environmental and health authorities because of their potential to release lethal biological toxins, in particular, microcystins (MCs) produced from cyanobacterial HABs. Current monitoring methods employing on-site sampling followed by in-lab analysis of HAB toxins (direct micro-observation) are neither sustainable nor practical to meet the vast spatial and temporal measuring needs. Dr. Park will collaborate with environmental engineers, microbiologists, and sensor node fabrication experts to study methods to monitor, in real time, the level of MCs in situ using a wireless sensor network (WSN). Dr. Park will be responsible for devising the WSN's architecture and developing its MAC protocol.

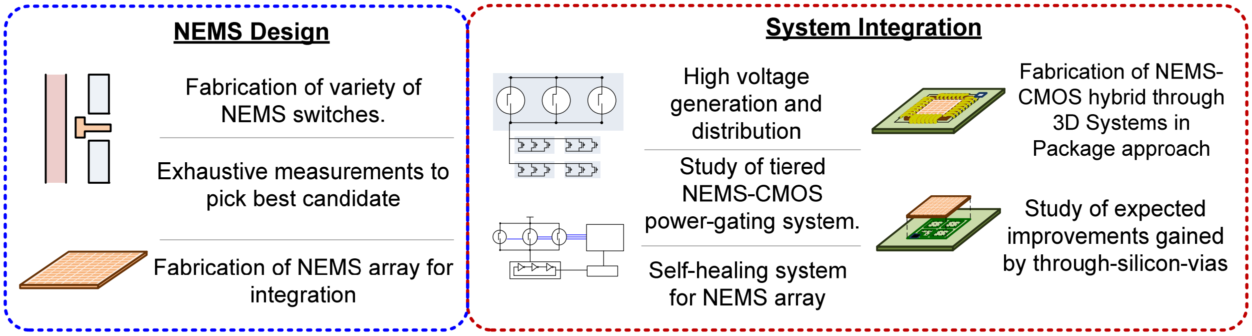


Outdoor Cognitive Radio Network Testbed

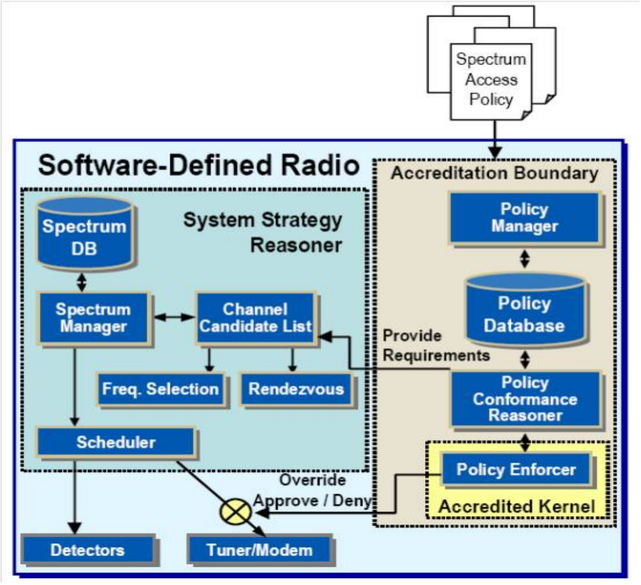
CESCA member Dr. Jerry Park and Dr. Jeff Reed, Director of the Wireless@Virginia Tech group, recently started a project entitled "Outdoor cognitive radio network testbed". This project is sponsored by the Office of Naval Research (ONR) through a grant totaling $260,400. This project aims to enhance the existing VT Cognitive Radio Network Testbed (CORNET) by building an Outdoor Cognitive Radio Network Testbed (O-CORNET), which will provide a field trial system for testing and evaluating real-world outdoor scenarios. O-CORNET will consist of 15 fixed outdoor radio nodes and 2 additional mobile outdoor nodes that will be installed on Virginia Tech's main campus in Blacksburg, VA. O-CORNET combined with the original VT-CORNET will create a unique testing environment that no other testbed offers. The outdoor nodes will enable researchers to test their radio systems' and protocols' performance as they move in and out of buildings, and roam the campus at varying speeds.

SePAC and VTMEMS Labs Join Forces to Build a Hybrid NEMS-CMOS Design

The steady rise in leakage power over the last decade has made low-power design an exceedingly difficult problem mainly because attempts to control leakage power tend to negatively impact performance and switching energy. For devices with long idle periods that are leakage-dominant, power gating has emerged as a popular technique for combating idle-leakage. The industry standard approach for power gating with on-die transistors has major drawbacks including residual off-state leakage, which still forces designers to resort to leakage control measures such as high threshold voltages. Leyla Nazhandali (CESCA member) and Masoud Agah (director of VTMEMS Lab) are set to solve this dilemma by using Nanoelectromechanical Systems (NEMS) switches. Their recently NSF funded project intends to thoroughly investigate all aspects of CMOS-NEMS integration. NEMS switches will be designed and developed that are specially targeted for effective power gating. The on-chip control circuitry will also be developed and tested, which includes a high-voltage generation system and a self-healing controller that can gracefully handle switch failure. Furthermore, 3D integration techniques will be evaluated for the integration of the NEMS switches with the CMOS die in such a way that power-network resistance and capacitance is minimized. The final product is a fabricated CMOS-NEMS hybrid that would allow us to conclusively determine the effectiveness of NEMS-based power gating.

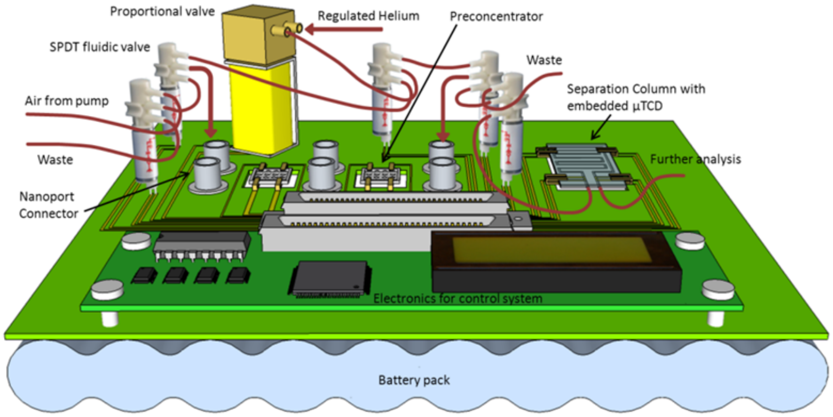

NEMS Design
Fabrication of variety of NEMS switches.
Exhaustive measurements to pick best candidate
Fabrication of NEMS array for integration
System Integration
High voltage generation and distribution
Study of tiered NEMS-CMOS power-gating system.
Self-healing system for NEMS array
Fabrication of NEMS-CMOS hybrid through 3D Systems in Package approach
Study of expected improvements gained by through-silicon-vias

Cognitive Radio Development



Drs. Michael Buehrer and Jerry Park recently started a Defense Advanced Research Projects Agency (DARPA)-sponsored project entitled "Cognitive radio development". The primary goal of the project is to design, develop, and implement waveforms that are resilient to various types of interference. The Virginia Tech researchers will collaborate with researchers from Lockheed Martin to develop the waveforms. The waveforms will incorporate various techniques at both the PHY and MAC layers to counter the effects of harmful interference, and will take advantage of the intelligence and spectrum agility of cognitive radios.

Clean Air for Workers



An interdisciplinary team of researchers: Linsey Marr (Civil and Environmental Engineering), Masoud Agah (Electrical Engineering) and Leyla Nazhandali (Computer Engineering) are the recipients of a research grant from National Institute of Safety and Health (NIOSH). The goal of the project is to develop a smart portable gas analyzer that can be used to measure hazardous air pollutants in (near) real-time in transportation-related and other workplaces. It can replace cumbersome sampling methods that must be followed by costly analysis in a laboratory. This programmable system is small enough that it can easily be worn to provide a measure of personal exposure to hazardous air pollutants.

Faculty Highlights

Schaumont was invited to give a talk at Qualcomm, San Diego, as part of their Short Subject in Security series. The talk discussed recent progress in Microprocessor-based Hardware Security. In recent years, 5 of Schaumont's graduates have joined Qualcomm.

Schaumont received the College of Engineering Dean's Award for Teaching Excellence, for his course on Hardware/Software Codesign as well as other computer engineering courses.

Schaumont is Track Chair for a special topic on Secure Systems for the 2013 Design Automation and Test in Europe Conference. The session will include papers in design methods and design of secure hardware and software.

Abbott gave a presentation at the University of Notre Dame in September, at the graduate seminar for their Department of Computer Science and Engineering. The title of the talk was “Temporal analysis of fingerprint impressions with live-scan systems.”

Abbott was invited to participate in a panel session at last June’s conference of the National Institute of Justice, which is held annually in Arlington, Virginia. Abbott described recent progress in fingerprint feature extraction and analysis. The NIJ-sponsored research has been conducted jointly with CESCA member Michael Hsiao, and with other collaborators.

Nazhandali is the guest editor for special issue of IEEE transaction on Design and Test of Computers. The focus of the issue is on Trusted System-on-Chip with Untrusted Components.

Student News

Who graduated in Spring 2012?

- Abhranil Maiti, *A Systematic Approach to Design an Efficient Physical Unclonable Function* (Ph.D.), Advisor: Patrick Schaumont, Next move: Intel Corporation (Hilsboro, OR)
- Alton Davis, project: *Visual projects and plans for freshman programming in computer engineering* (MEng), Advisor:Sandeep Shukla
- Eric Xu Guo, *Secure and Efficient Implementations of Cryptographic Primitives (Ph.D.), Advisor*: Patrick Schaumont, Next move: Qualcomm (San Diego, CA)
- Daniel Ali, *Scalable Parameter Management using Case-based Reasoning for Cognitive Radio Applications* (MS), Advisor: Jung-Min "Jerry" Park, Next move: KeyW Corp.
- Jihoon Jeong, *Low Power Merged LNA and Mixer Design for Medical Implant Communication Services* (MS), Advisor: Dong Ha
- Lalleh Rafeei, *Fast Approximation Framework for Timing and Power Analysis of Ultra-Low-Voltage Circuits* (MS), Advisor: Leyla Nazhandali
- Nevedetha Narayanan, MEng, Advisor: Michael Hsiao, Next move: Qualcomm
- Preeti Kumar, project: *Automated extraction of polychronous models from C Programs* (MEng), Advisor: Sandeep Shukla, Next move: Amazon
- Sarvesh Prabhu, *An efficient 2-phase strategy to achieve high branch coverage* (MS), Advisor: Michael Hsiao, Next move: continue Ph.D. at Virginia Tech
- Supratik Misra, *Efficient graph techniques for partial scan pattern debug and bounded model checkers* (MS), Advisor: Michael Hsiao,Next move: Intel Corp.
- Suvarna Mane*, Implementation of SCA-Resistant CPU and an ECDLP Engine on FPGA Platform* (MS), Advisor: Patrick Schaumont, Next move: Qualcomm (Raleigh, NC)
- Drumeel Bakshi, Techniques for seed computation and testability enhancement for logic Built-In Self Test (MS), Advisor: Michael Hsiao, Next move: Synopsys.
- Chuan Han, (PhD), Advisor: Yaling Yang, Next move: CISCO.

Internships

- Avinash Desai, Intel
- Dilip Murali, Qualcomm
- Sarvesh Prabhu, Intel
- Rashmi Moudgil, Nvidia
- Meeta Srivastav, USC Information Sciences Institute
- Dinesh Ganta, Intel
- Jingyao Zhang, Robert Bosch LLC, Research and Technology Center
- Ting Wang, Amazon

Publications

- Huy Nguyen and Michael S. Hsiao, *"Sequential equivalence checking of hard instances with targeted inductive invariants and efficient filtering strategies,"* to appear in *Proceedings of the IEEE High Level Design Validation and Test Workshop*, November 2012.
- Min Li, Kelson Gent, and Michael S. Hsiao, *"Design validation of RTL circuits using evolutionary swarm intelligence,"* to appear in *Proceedings of the IEEE International Test Conference*, November, 2012.
- Gyanendra Shrestha and Michael S. Hsiao, *"Ensuring trust of third-party hardware design with constrained sequential equivalence checking,"* in *Proceedings of IEEE International Conf. on Technologies for Homeland Security*, Nov. 2012.
- Dhrumeel Bakshi, Sarvesh Prabhu, and Michael S. Hsiao, *"LBIST Reseeding With a New SMT-based Chainability Analysis,"* in *SRC TECHCON*, September 2012.
- Sarvesh Prabhu, Michael S. Hsiao, Loganathan Lingappan and Vijay Gangaram, *"A SMT-based diagnostic test generation method for combinational circuits,"* in *Proceedings of the IEEE VLSI Test Symposium*, April 2012.
- Kameshwar Chandrasekar, Supratik K. Misra, Sanjay Sengupta, and Michael S. Hsiao, *"A scan pattern debugger for partial scan industrial designs,"* in *Proceedings of the IEEE Design Automation and Test in Europe Conference*, March 2012.
- Min Li and Michael S. Hsiao, *"RAG: An efficient reliability analysis of logic circuits on graphics processing units,"* in *Proceedings of the IEEE Design Automation and Test in Europe Conference*, March 2012.
- Nathan J. Short, A. Lynn Abbott, Michael S. Hsiao, and Edward A. Fox, *"Reducing descriptor measurement error through Bayesian estimation of fingerprint minutia location and direction,"* in *IET Biometrics,* vol. 1, no. 1, March 2012, pp. 82-90.
- Miron Abramovici, Dakshi Agarwal, Swarup Bhunia, Paul Bradley, Michael S. Hsiao, Jim Plusquellic, and Mohammad Tehranipoor, *"Protection against hardware trojan attacks: towards a comprehensive solution,"* to appear in *IEEE Design & Test of Computers,* 2012.
- Chuan Han and Yaling Yang, Understanding the Information Propagation Speed in Multihop Cognitive Radio Networks , *IEEE Transactions on Mobile Computing*, to appear.
- Bo Gao, Jungmin Park, Yaling Yang, A Taxonomy of Coexistence Mechanisms for Heterogeneous Cognitive Radio Networks Operating in TV White Spaces , *Wireless Communications Magazine*, Aug 2012
- Ting Wang and Yaling Yang, "Enhancing Wireless Communication Privacy with Artificial Fading," *9th IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS)*, 2012.

- Jingyao Zhang, Srikrishna Iyer, Patrick Schaumont, and Yaling Yang Simulating Power/Energy Consumption of Sensor Nodes with Flexible Hardware in Wireless Networks , *Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*, 2012
- Bo Gao, Jung-Min Park, and Yaling Yang, "Uplink Soft Frequency Reuse for Self-Coexistence of Cognitive Radio Networks Operating in White-Space Spectrum , *31st Annual IEEE International Conference on Computer Communications (IEEE INFOCOM 2012)*, 2012.
- M. Taha, P. Schaumont, "A Novel Profiled Attack in the Presence of High Algorithmic Noise," International Conference on Computer Design (ICCD 2012), September 2012.
- S. Mane, M. Taha, P. Schaumont, "Efficient and Side-Channel-Secure Block Cipher Implementation with Custom Instructions on FPGA," International Conference on Field Programmable Logic and Applications (FPL 2012), August 2012.
- A. Maiti, P. Schaumont, "A Novel Microprocessor-intrinsic Physical Unclonable Function," International Conference on Field Programmable Logic and Applications (FPL 2012), August 2012.
- M. Srivastav, X. Guo, S. Huang, D. Ganta, M. B. Henry, L. Nazhandali, and P. Schaumont, "Design and Benchmarking of an ASIC with Five SHA-3 Finalist Candidates," Elsevier Microprocessors and Microsystems - Embedded Hardware Design (Special Issue on "Digital System Security and Safety"), 2012.
- J. Zhang, S. Iyer, P. Schaumont, Y. Yang, "Simulating Power/Energy Consumption of Sensor Nodes with Flexible Hardware in Wireless Networks," 9th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), 2012.
- L. Judge, P. Schaumont, "A Flexible Hardware ECDLP Engine in Bluespec," Special-Purpose Hardware for Attacking Cryptographic Systems (SHARCS 2012), Washington, DC, March 2012.
- R. Chen, J. Park, and K. Bian, “Robustness against Byzantine failures in distributed spectrum sensing,” Elsevier Computer Communications, to appear.
- K. Bian and J. Park, “Maximizing rendezvous diversity in rendezvous protocols for decentralized cognitive radio networks,” IEEE Transactions on Mobile Computing, 2012, to appear.
- B. Bahrak, A. Deshpande, and J. Park, “Spectrum access policy reasoning for policy-based cognitive radios,” Elsevier Computer Networks, vol. 56, issue 11, 2012, pp. 2649–2663.
- J. H. Reed, J. T. Bernhard, and J. Park, “Spectrum Access Technologies: The Past, the Present, and the Future (invited paper),” Proceedings of the IEEE, Vol. 100, Special Centennial Issue, May 2012, pp. 1676–1684.
- B. Bahrak, J. Park, and H. Wu, “Ontology-based spectrum access policies for policy-based cognitive radios,” IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), Oct. 2012.

Book Chapters

- A. Maiti, V. Gunreddy, P. Schaumont, "A Systematic Method to Evaluate and Compare the Performance of Physical Unclonable Functions," Chapter 11 in "Embedded System Design with FPGAs," Eds. P. Athanas, D. Pnevmatikatos, N. Sklavos, Springer 2012, ISBN 978-1-4614-1361-5.

Editor of Conference Proceedings

- E. Prouff, P. Schaumont, Cryptographic Hardware and Embedded Systems - CHES 2012. 14th International Workshop. Leuven, Belgium, September 2012. Springer Lecture Notes on Computer Science (LNCS), Vol 7428.
- A. Maiti, V. Gunreddy, P. Schaumont, "A Systematic Method to Evaluate and Compare the Performance of Physical Unclonable Functions," Chapter 11 in "Embedded System Design with FPGAs," Eds. P. Athanas, D. Pnevmatikatos, N. Sklavos, Springer 2012, ISBN 978-1-4614-1361-5.

Editor of Conference Proceedings

- E. Prouff, P. Schaumont, Cryptographic Hardware and Embedded Systems - CHES 2012. 14th International Workshop. Leuven, Belgium, September 2012. Springer Lecture Notes on Computer Science (LNCS), Vol 7428.