Center for Embedded Systems for Critical Applications

VirginiaTech
Invent the Future

CESCA Newsletter
Center for Embedded Systems for Critical Applications

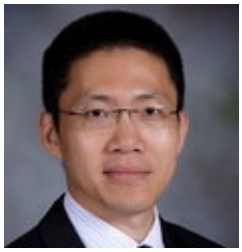
CESCA • 302 Whittemore Hall • Dept. of ECE • Virginia Tech • Blacksburg • 24061 • USA

September 2013▪ No.010

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.

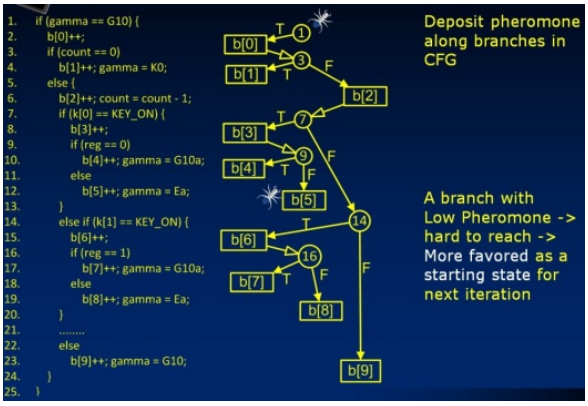
Awards and Honors

Chao Wang received the ONR YIP Award



Dr. **Chao Wang** received the prestigious Office of Naval Research (ONR) Young Investigator Program (YIP) award in May 2013. The title of his proposal is “Automated Software Model Generation for Identifying and Mitigating Concurrency Vulnerabilities.” The YIP award seeks to identify and support faculty members who are early in their careers and who show exceptional promise for doing creative research. The award is extremely competitive -- ONR made only 16 awards in 2013. The three-year $510,000 grant will support Dr. Wang develop new methods and software tools for improving the reliability and security of concurrent software running on multicore computers.

Best Student Paper Award at International Test Conference



Min Li, **Kelson Gent**, and **Michael Hsiao**, authors of the 2012 paper entitled "Design Validation of RTL Circuits Using Evolutionary Swarm Intelligence" received the Best Student Paper Award (best paper with student as primary author) at 2013 ITC, the flagship hardware testing conference. In this paper, a bio-inspired heuristic is used for design validation and functional test generation. The approach combines Ant Colony Optimization (ACO) with an evolutionary search for improved search capability for circuits described at the register-transfer level (RTL). The goal is to reach 100% branch coverage of the RTL code. By trimming highly visited branches from the search, the search can focus on those corner cases by tailoring the swarm-intelligence algorithm to find the way to reach them. New states have been discovered using the approach, allowing for high coverages. For many circuits, one to two orders of magnitude speedups were achieved over existing methods. This work is supported in part by an NSF grant.

Awards at CESCA Day 2013

The 4th annual CESCA Day was held on a sunny Saturday in April. The day consisted of research presentations, poster sessions, and other events. The keynote address was provided by Kevin Bowyer, Department Chair of Computer Science & Engineering at the University of Notre Dame. Dr. Bowyer's talk discussed the effect of contact lenses on Iris Recognition Accuracy in biometrics. An online video of his talk is available on the CESCA Website.

On CESCA Day, the students in CESCA present their research results through poster presentations. We discussed 27 posters covering a broad range of areas in image processing, hardware security, test and verification, chip design, side-channel analysis, cryptographic engineering, networking, and software radio.

This year, for the first time, the CESCA Faculty organized the CESCA Awards. In order to recognize academic excellence, students can compete for awards in multiple categories. This years, there were 4 award categories.

- The CESCA Best Presentation was awarded to the student which could make the best 10-minute summary presentation of a conference paper presented in the past year. The award is organized as a presentation competition among students. This year, the award went to **Aydin Aysu** (Advisor Schaumont) for his presentation on 'Low-Cost and Area-Efficient FPGA Implementations for Lattice-Based Cryptography'.
- The CESCA Outstanding Student Award was given to any student who has published 5 first-author peer-reviewed conference or journal papers. This year, two students won an award in this category: **Meet Srivastav** (Advisor Nazhandali) and **Beghnam Bahrak** (Advisor Park).
- The CESCA Best Poster Award was given to the student who made the best pitch during the poster presentations at CESCA Day 2013. This award was decided by voting among CESCA faculty. The best poster for CESCA Day 2013 was presented by **Rashmi Moudgil** (Advisor Nazhandali) for the poster 'A Statistical and Circuit-based Technique for Detection of Counterfeits in Existing ICs'.
- The CESCA Service Award was awarded to a student who has shown exceptional service to CESCA during the past year. The award was decided by vote among CESCA Faculty, who selected **Mahesh Nanjundappa** (Advisor Shukla) for his service in recording and digitizing the CESCA Seminars.

Aydin Aysu
Best Presentation Award

Meet Srivastav,
Outstanding Student Award

Beghnam Bahrak
Outstanding Student Award

Rashmi Moudgil
Best Poster Award

Mahesh Nanjundappa
Service Award

In summary, CESCA Day 2013 was a very successful event, and it enabled CESCA faculty and students to network together. Our **CESCA Day 2014** will be scheduled on 19 April 2014 in Claytor Lake State Park (Dublin, VA). We will gladly invite external sponsors or interested attendees from industry - please let us know by email (schaum@vt.edu)!

From the Director's Desk

We live in times of amazing technological breakthroughs. NASA just announced the Voyager I entered the interstellar space. This technological achievement has produced mind-boggling numbers. Voyager I was launched in 1977, when our current CESCA students weren't born yet. The spacecraft is at 125 times the distance between the sun and the earth, and its communications take 17 hours to reach us. Its computers are far more modest of what we think of today as a *critical embedded system*. Voyager I relies on a set of three distributed computers with 4K memory, built using 150 low-power TTL circuits and running 80,000 cycles per second (a fascinating overview of early-spaceflight computing is on http://history.nasa.gov/computers/contents.html). Yet today, 35 years later, these computers travelled further than any other manmade object has ever been, and everyday they bring new insights into the final frontier.

In those 35 years, the voyage of technology on earth has been at least as groundbreaking. Today, our embedded systems contain millions of gates, and they are assembled in networks of thousands of computers. I feel genuinely humbled by the endless creativity and imagination of humankind. Our technologies and our engineering feats have something truly transformative to them, constantly improving the human condition. Engineering education has become a transformative process as well. In the medieval guilds, a barrel-maker was in the business of training another barrel-maker, and a mason was in the business of training another mason. Today, modern engineering faculty is in the business of creating engineers who will be able to outperform them technologically. A graduating engineer is state-of-the-art technology in every sense of the word, capable of moving beyond the limits of knowledge and technology.

CESCA is in the privileged position of hosting 37 of tomorrow's engineers (26 PhD and 11 MS). That is a 10% increase over last year. The past year has been very productive for both the CESCA students and their advisors. We have multiple new projects, new courses, and this newsletter will give you a sample of our recent achievements and activities.

We also have thoroughly reworked our website to provide easy access to data on our graduating students, our latest research results, and our publications

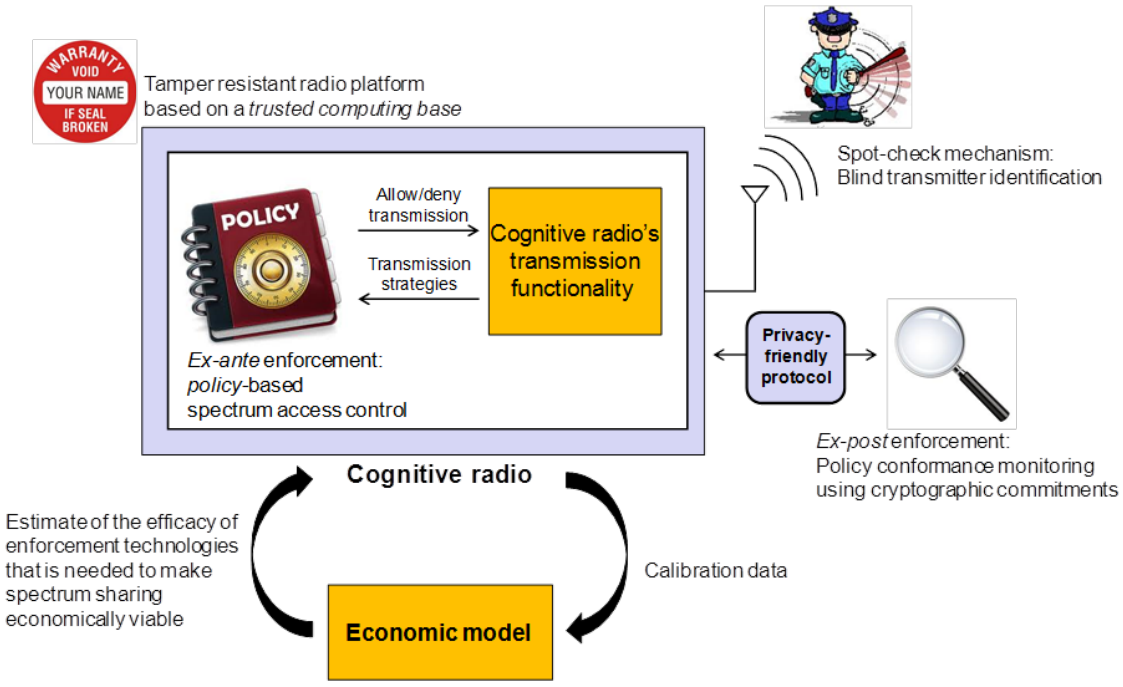
(http://www.cesca.centers.vt.edu/). In addition, most of the CESCA seminars from last year can be easily accessed online.

Since many of our graduates eventually transition to industrial research labs, we wish to nurture our relationship with industry. CESCA has a model in place to help industry to benefit in a direct way from CESCA know-how - **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. Full details of the CESCA Affiliate Program may be found at the CESCA website.

Let me wish everyone, the CESCA students, faculty, and especially you, the reader, a great year and a fantastic voyage in 2013-2014.
Patrick Schaumont
CESCA Director

Featured News

A new project in trustworthy spectrum sharing



Mobile data traffic is increasing some 450 times between 2005 and 2015. In fact, the spectral efficiency has doubled every 18 months or greater than 112 times since Italian inventor Guglielmo Marconi started playing with radio waves in the late 1800s.

The needed spectrum to carry this additional communications traffic exists, but government-regulated allocations has some of this space off-limits to wireless providers.

An answer is to share the use of the communications spectrum superhighways in the sky that already exist.

“However, one of the critical challenges that needs to be addressed for spectrum sharing is the problem of spectrum security and enforcement,” said **Jung-Min “Jerry” Park**, Virginia Tech associate professor of electrical and computer engineering. “The primary concern is the interference experienced by primary users due to rogue transmissions by maliciously intended secondary users when the two groups operate in the same band.”

To counter this problem, Park and his colleague **Patrick Schaumont**, also an associate professor of electrical and computer engineering, Michelle Connolly, professor of practice in economics at Duke University, and Nelson Sa, assistant professor of economics at Vassar College, are the principal investigators on a new $1.2 million award from the National Science Foundation’s Secure and Trustworthy Cyberspace program. Virginia Tech holds the largest portion of this interdisciplinary funding, receiving approximately $898,000 of the overall budget.

Their goal is to make trustworthy spectrum sharing technically and economically viable.

The primary users of these crowded, yet invisible superhighways are the license holders or in the case of federal government users, incumbents of a given spectrum. Park politely considers the secondary users “opportunistic”.

However, the threat from the opportunists is serious for two reasons, he explained. First, interference caused by rogue transmitters will undermine the advantages of spectrum sharing and seriously hinder its world-wide adoption. Second, cognitive radios that make spectrum sharing possible can be used to launch very destructive jamming attacks.

“Counter measures against these threats can be classified into two enforcement approaches: ex-ante or preventive and ex-post or punitive enforcement. Our research is focused on studying the key mechanisms in both of these enforcement approaches,” Park said.

Among his many research projects, Park has previously worked on a privacy enhancing technology to protect children’s online privacy, problems of spectrum etiquette in cognitive radio networks, and secure spectrum sensing techniques.

Schaumont is a recipient of an NSF CAREER award to work on hardware and software co-design for secure embedded systems. He has addressed the design of tamper-resistant and efficient cryptography in embedded systems, and constructed a database to support research in secure circuit identifiers.

Tackling the economic considerations of spectrum security and enforcement will be Connolly and Sa. Connolly is a former two-term chief economist for the Federal Communications Commission. Sa is an economic theorist who specializes in industrial organization and economic growth.

The grant will be extended over a four-year period.

Research Highlights

Design of Low Power, Scalable-Throughput Many-core DSP systems at Near Threshold Voltages

A 90 nm IBM process chip that was designed by CESCA members, **Meeta Srivasta** (Ph.D. candidate) and Dr. **Leyla Nazhandali** (faculty) has been successfully tested. The chip that has been extensively tested by two undergraduate researchers, **Kyle Stegner** and **Mohammed Ehteshamuddin**, is providing very interesting insights into design of multi-core homogeneous DSPs in the presence of process variation.

Voltage scaling has been a prevalent method of saving energy for energy-constrained applications. However, the current technology trends which shrink transistors sizes exacerbate process variation effects in voltage scaled systems. Large variations in transistor parameters result in high variation in performance and power across the chip. These effects, if ignored at the stage of designing, will result into non-optimal behavior when deployed in the field. This is especially the case for multi-core DSP designs, where multiple cores will need to operate at the same frequency to finish a desired task. In our method, the number of cores and their operating voltage are selected such that a desired throughput is met while minimizing the power consumption, all in the presence of process variation.

In the first phase of project, we performed an extensive study of such system based on simulation, which resulted in two conference and one IEEE journal papers. In the second phase, An ASIC chip was designed and fabricated using 90nm IBM process library to verify the findings of the first phase. The chip contains a total of 16 cores, 8 homogeneous cores of 16-bit multiplier and 8 homogeneous cores of 8-bit FIR filter. Layout of the chip is shown in Fig. (A). The chip works on two different voltage domains, one voltage caters to all the cores and the other voltage domain is connected to the common controller. Voltage to the core can be changed from sub-threshold voltage to super threshold voltage (0.35v to 1.4v). The chip has 4 programmable on-chip clocks capable of generating a frequency of 9 MHz to 1 GHz range. Setup for testing the chip is shown in Fig.(B). We are working on several publications based on the chip measurement results. Our analysis shows that using our method, up to 30% power reduction can be expected compared to a base design.

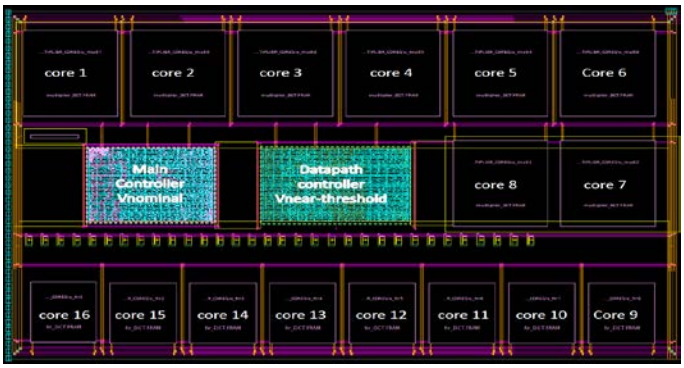


Fig.(A) Chip Layout

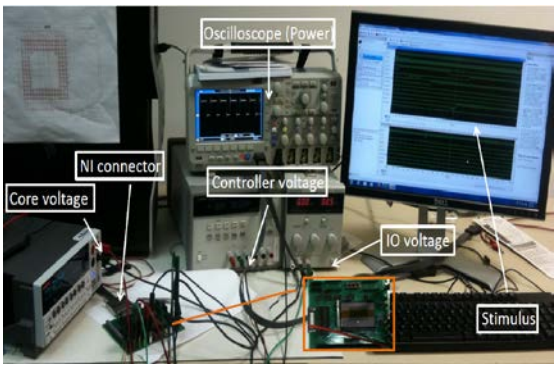
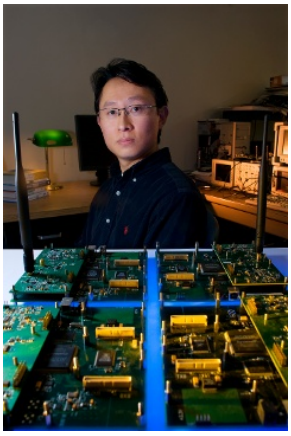


Fig.(B) Chip test setup.

New Projects

Virginia Tech and partner universities to study problems in broadband wireless access and security



Virginia Tech is part of a five university member group being funded by the National Science Foundation to expand access to and security of the nation's broadband wireless network. The university consortium will work with private industry as it carries out research.

The consortium is the latest effort of the Virginia Tech College of Engineering as it remains a leading national research institute of wireless technologies and cyber security, critical to the nation's economy and security.

Virginia Tech will receive $300,000 during a five-year period for its research efforts in the public/private consortium known as the Broadband Wireless Access & Applications Center, or BWAC for short. Joining Virginia Tech in the consortium are Auburn University, Notre Dame University, the University of Arizona, and the University of Virginia.

The group was formed this past March and will operate as an Industry-University Cooperative Research Center, working with and receiving additional funding from industry. The group's research efforts will be overseen by the National Science Foundation.

Serving Virginia Tech's sire director for the center will be **Jung-Min "Jerry" Park**, an associate professor in the Bradley Department of Electrical and Computer Engineering. He will be joined by faculty members Jeffrey H. Reed, holder of the Willis G. Worcester Professorship; R. Michael Buehrer, professor; Luiz DaSilva, professor; Carl Dietrich, research associate professor; Allen MacKenzie, associate professor; and William Tranter, Bradley Professor of Communications; all of electrical and computer engineering.

Teaming with industry partners, the Broadband Wireless Access & Applications Center will pursue large-scale research programs dedicated to designing flexible, efficient, and secure wireless networks that are both novel and meet broadband communication needs for business and homes, said Park. An Industry-University Cooperative Research Center status opens doors for academics and industry experts to share research and in-development technologies, and provide real-life in-lab work experience to students conducting research at the member universities, Park said. Twenty industry partners are planned.

Each university in the center site has a specific research thrust where in-house experts will focus on individual areas of the larger project. Park, Reed, and their collaborators will study problems in spectrum enforcement, security, and privacy in spectrum sharing; mobility support for opportunistic spectrum access; co-design and coexistence of heterogeneous wireless systems; and security issues in cognitive radio networks.

Leading the full consortium is Tamal Bose, head of the University of Arizona's Department of Electrical and Computer Engineering who previously worked as a professor with the Bradley Department of Electrical and Computer Engineering at Virginia Tech, and served as associate director of Wireless@VT, which is headed by Jeffrey Reed.

Virginia Tech has long been well-known for its research into wireless technology, dating back to the 1960s with development of technology that has served as the basis for such companies as Direct TV, Iridium Satellite, and Globalstar.

Researchers Study Privacy Issues in Database-Driven Spectrum Sharing

The role of spectrum as an important economic growth engine was brought forth in the recently announced National Broadband Plan (NBP) as well as in the President's Council of Advisors on Science and Technology (PCAST) report entitled "Realizing the Full Potential of Government-Held Spectrum to Spur Economic Growth". A broad range of innovative spectrum access technologies and policies will need to be developed to realize the recommendations of the PCAST report, which includes the ambitious goal of sharing underutilized Federal spectrum and identifying 1,000 MHz of Federal spectrum as part of an effort to create "the first shared-use spectrum superhighways". To realize the vision described in the NBP, the National Telecommunications and Information Administration (NTIA) is currently studying the viability of opening up all or parts of the 1755–1850 MHz band, which is currently used exclusively by the Dept. of Defense (DoD), to commercial systems to enable spectrum sharing.

In the shared spectrum access model, a heterogeneous mix of wireless systems of differing access priorities, QoS requirements, and transmission characteristics need to coexist without causing harmful interference to each other. In this model, secondary users identify fallow spectrum by accessing a geolocation database that is constantly updated with the primary users' spectrum utilization information. One of the critical challenges that need to be addressed to realize the shared access model is addressing the security and privacy issues. This problem is especially paramount when federal government systems, including DoD systems, coexist with commercial systems in the same spectrum bands. In such scenarios, federal government users are primary users and private users as secondary users.

A group of researchers lead by **Jung-Min "Jerry" Park** (PI, Associate Professor in ECE) and **Jeffery Reed** (co-PI, Willis G. Worcester Professor in ECE) are investigating the aforementioned privacy issues in the context of spectrum sharing. This research is being funded by Motorola Solutions. The project's primary goal is to develop mechanisms and techniques for an *obfuscated* geolocation database that can enable the coexistence of primary and secondary users while addressing sensitive privacy issues.

New Project Related to Wildlife Management

CESCA faculty member **Lynn Abbott** and CESCA student **Ahmed Ibrahim** are collaborating with Prof. **Jeff Reed** at Wireless@VT on a new project related to image capture for wildlife management. The first phase of the project is develop an integrated imaging system that tightly couples an infrared camera with an Android device. Software developed by CESCA will allow the Android device to control a commercially available FLIR camera, capturing images and supplementing those files with additional sensor "metadata" from the Android platform. For

example, GPS locations can be captured in sync with the images, to facilitate better insights into wildlife behavior. Infrared imaging is especially well suited for this application because many species of interest are nocturnal, and the animals can be seen in infrared images in low-light conditions when visible-light imaging is not feasible. Sponsored by the Dept. of Defense, the project is intended for use in wildlife management on military bases.

Teaching Innovation

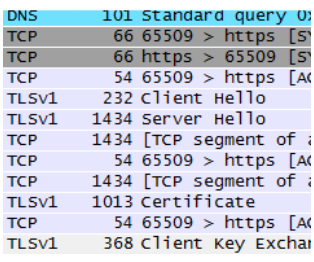
Intel Sponsors Embedded Curriculum Development

Patrick Schaumont, like other CESCA faculty members, is actively developing novel curriculum for the next generation of computer engineers. Over the past few months, Schaumont received support from Intel in the form of novel, state-of-the-art equipment as well as student support, to develop new courses.

In spring 2013, Intel donated a set of BIS-NORCO 6630 computers, which are Atom N2800-based embedded computers for industrial and kiosk applications. The computers have been used in Schaumont's "Handheld Computer Security" course, a course on cryptographic engineering. The Atom processor is a low-power processor with vector-instruction capabilities (SSE2). During the course, students evaluated the capabilities of the Atom processor to support modern public-key cryptographic protocols. They developed a vectorized version of a long-integer multiplication algorithm, a fundamental component of public-key operations. The students demonstrated an accelerated version of prime-field elliptic curve signature algorithm. The results will be presented at the upcoming IEEE Conference on High-Performance Embedded Computing in Boston.

In fall 2013, Intel donated a set of Terasic DE2i-150 boards, which combine a high-end Altera Cyclone IV FPGA with an Atom Processor. These boards are part of an effort by Intel to establish an embedded curriculum. Schaumont is using these boards to develop assignments for his course on "Hardware-Software Codesign," taken by 57 graduate and undergraduate students. Schaumont also received financial support for a graduate student. The objective of this project is to create publicly accessible content for this curriculum. CESCA is hosting a dedicated website which will collect the results, on http://rijndael.ece.vt.edu/de2i150/
This project is a good example of how industry and academia can collaborate, and use tomorrow's technology to train students.

CESCA Faculty Collaborate on Cybersecurity Curriculum Development



CESCA Faculty Members **Jung-Min "Jerry" Park** and **Patrick Schaumont** are collaborating with other faculty members in ECE and CS to establish a curriculum oriented towards cybersecurity. For this purpose, Park and Schaumont each developed a course that is part of a comprehensive graduate-level education.
Park is working on ECE 5560, Fundamentals of Information Security. This course covers fundamental principles of information security as well as the relevant mathematical concepts. The course is being offered in fall 2013 for the first time in its revised form. The covered topics include classical

ciphers, abstract algebra, number theory, symmetric-key ciphers, AES, cipher modes of operation, asymmetric-key ciphers, cryptographic hash functions and message authentication codes, and elliptic curve cryptography and cryptosystems. The course also provides an overview of some of the applications and standards that are relevant to network and computer security.

Schaumont will develop ECE 55XX, Cryptographic Engineering. This course covers the implementation of cryptographic operations and protocols in contemporary computing platforms ranging from handheld computing devices to servers. The course will be offered in spring 2014. Topics include mapping of cryptographic operations, evaluation and optimization of performance and implementation cost, analysis of security against brute-force cryptanalysis and implementation-level attacks, design of countermeasures against implementation-level attacks, security-testing procedures, and architectures to support a trusted computing base.

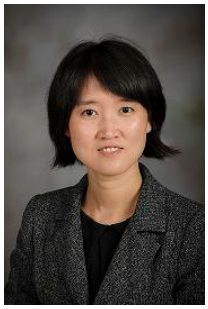
Additional courses in network security and software security are being developed in collaboration with the Computer Science Department. These new and/or improved courses cover an important area of national need, and they ensure that our students will be well prepared for their research careers.

Faculty Highlights

Leyla Nazhandali named Teacher of the Week (9/15/ 2013)

The Center for Instructional Development and Educational Research (CIDER) has recognized **Leyla Nazhandali** for innovative teaching methods that stimulate active participation from students, and for original outreach to attract high school students to the computer engineering curriculum. Dr. Nazhandali is a genuinely gifted teacher in the electrical and computer engineering department. She teaches computer architecture classes to sophomores as well as graduate students, and is known as a lively and engaging teacher. Her office hours are always crowded with students, and she regularly has to move the whole group into a separate meeting room to discuss and to make sure that everyone has a chance to meet. Her teaching style is a middle ground between "straight lecturing" and "inverted classroom." In this model, the students first learn for half of the class about a new topic. At the end of that, Dr. Nazhandali gives them a problem to work on, and the whole class wrestles with it. The problem is left unfinished so that the students can "sleep on" the material and hopefully work on it independently at home. At the next class, there is again half a lecture of new material, and then the problem from the previous lecture is finished. Besides attracting freshman to computer engineering, Dr. Nazhandali has extensively participated in outreach and summer camp activities associated with CEEDS. In 2008 and 2009, she participated in Women in Computing Day, which is the biggest event organized each year by the Association for Women in Computing.

Yaling Yang named Scholar of the Week (4/22/2013)



Yaling Yang, one of the CESCA faculty members, has been recognized as Scholar of the Week by the Virginia Tech Office of the Vice President for Research. She was recognized for her work with wireless network modeling, design, and security. In addition, Yang studies network resource management and network quality of service, which refers to the ability to prioritize applications, users, or data flows, or to guarantee a certain level of performance to a data flow. One of her ongoing projects sponsored by the National Science Foundation (NSF) involves hardware-based security solutions for Software Defined Radio (SDR). SDR technology has the flexibility of implementing a large part of physical layer functions in software. It is one of

the major technologies that will provide broadband services to millions of U.S. residences. However, unlike conventional radio, whose frequency 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 sufficient to close the myriad of potential software security loopholes and themselves often become targets of the malware. The objective of this project is to design an effective hardware-based SDR integrity assessment and behavior regulation device named SDR shield.

Chao Wang named Outstanding New Assistant Professor

Chao Wang was named the Outstanding New Assistant Professor by the College of Engineering at Virginia Tech in April 2013. The award recognizes tenure-track faculty members who have performed exceptionally well in scholarship, research, and teaching in the first three years of their service at Virginia Tech. In Dean Benson's speech, Dr. Wang was noted for the following achievements: he had secured a total of $1.7 million in external funding, with a personal share of $1.2 million; he had received the prestigious NSF CAREER award in 2012; he was an effective teacher, evident from his exceptional teaching evaluations and many of the "Thank a Teacher" notes that he received from his students; and he had served on the program committees of many flagship conferences of his field.

Patrick Schaumont named College of Engineering Faculty Fellow

Patrick Schaumont was recognized as a College of Engineering Faculty Fellow, an award that carries an annual $5000 account for the next three fiscal years. Schaumont's research focuses on the efficient implementation of secure embedded systems, essential for the operation of critical structures such as banking, smart grids, and autonomous vehicles. His overall level of funding since joining the college in 2005 is $3.1 million with a personal share of $1.8 million. He has an NSF CAREER award, a National Institute of Standards and Technology grant and three industry contracts. He has published two books. These books are the basis for a course at Virginia Tech and several other universities.

Chao Wang visited industry labs for possible research collaboration

Chao Wang visited Fujitsu Laboratories of America, Inc. in Sunnyvale, California, Sandia National Laboratories in Livermore, California, and NASA's Ames Research Center in August 2013, to meet with colleagues and discuss possible collaboration in research. He also gave a talk on symbolic predictive analysis for improving the reliability and security of concurrent software at each of these organizations.

CESCA Training and Seminars

CESCA Seminars in Fall 2013

CESCA seminars are held on weekly basis during the semester, and are held in Lavery Hall 250 from 2:30PM-3:30PM on Fridays. The speakers are faculty members of CESCA, ECE, and Virginia Tech as well as external speakers, and cover a broad range of topics in electronic system design. The seminars are open to everybody. Please join us!

- 9/16/13: Michael Fowler, ECE Department, Virginia Tech, "Targeting Innovation for Defense Agencies through Sponsor Awareness"

- 9/27/13: Patrick Schaumont, ECE Department, Virginia Tech, “Don't talk to strangers (without authentication)”
- ***Upcoming 10/4/13***: Berk Sunar, Worcester Polytechnic Institute, " An FHE Implementation based on NTRU"
- ***Upcoming 10/11/13***: Bob Summer, Local entrepreneur.
- ***Upcoming 11/1/13***: Ayse Coskun, Boston University
- ***Upcoming 12/6/13***: Changhee Jung, CS Department, Virginia Tech

Student News & Highlights

New Students

- Moein Pahlavan Yali, PhD student
- Abhijit Sarkar, PhD student
- Kexiong (Curtis) Zeng, PhD student
- Sudeep Bhattarai, PhD student
- Yanzhi "Charles" Dou, PhD student

Summer Interns

- Lu Zhang (Ph.D. student): Fujitsu Laboratories of America
- Kelson Gent (Ph.D. student): Intel
- Arijit Chattopadhyay (M.S. student): Bloomberg
- Mahmoud Elbayoumi (Ph.D. student): IBM, TJ-Watson
- Vineeth Acharya (M.S. student): Intel
- Sharad Bagri (M.S. student): Qualcomm
- Shuchi Pandit (M.S. student): National Instruments
- Deepak Mane (M.S. student): LSI Logic
- Krishna Pabbuleti (M.S. student): CISCO

Recent Graduations

- Avinash Desai (M.S., advisor: Hsiao), Joined Intel.
- Ting Wang (Ph.D., advisor: Yang), Joined Google
- Jingyao Zhang (Ph.D., advisor: Yang), Joined Qualcom
- Lakshman Swaroop Babu (M.S., advisor: Yang), Joined CISCO
- Daniel R. Ali (M.S., advisor: Park), Joined Hexis Cyber Solutions, Inc.
- Kiran Adhikari, (M.S., advisor: Wang) Joined Intel
- Rashmi Moudgil, (M.S., advisor: Nazhandali) Joined Qualcomm

Publications

- A. Aysu, C. Patterson, P. Schaumont, "Low-Cost and Area-Efficient FPGA Implementations of Lattice Based Cryptography",*IEEE International Symposium on Hardware-Oriented Security and Trust (HOST 2013)*, Austin, TX, June 2013.
- A. Aysu, N. Ghalaty, Z. Franklin, M. Yali, P. Schaumont, "Digital Fingerprints for Low-Cost Platforms using MEMS sensors," *8th Workshop on Embedded Systems Security (WESS 2013)*, September 2013, Montreal.
- B. Gao, Y. Yang, J. Park, "Uplink Soft Frequency Reuse for Self-Coexistence of Cognitive Radio Networks," *Transactions On Mobile Computing*, to appear.
- D. Ali, J. Park, and A. Amanna, "A feature partitioning approach to case-based reasoning in cognitive radios," *International Conference on Cognitive Radio Oriented Wireless Networks (CROWNCOM)*, July 2013.
- D. Bakshi and M. S. Hsiao, *"*LFSR seed computation and reduction using SMT-based fault-chaining*,"* in *Proceedings of the IEEE Design Automation and Test in Europe Conference*, March, 2013.
- D. Mane, P. Schaumont, "Energy-Architecture Tuning for ECC-based RFID Tags", *9th Workshop on RFID Security (RFIDSec 2013)*, Graz, Austria, July 2013.
- F. Bélanger, R. E. Crossler, J. S. Hiller, J. Park, and M. Hsiao, "POCKET: A Tool for Protecting Children's Privacy Online," *Elsevier Decision Support Systems* (Journal), vol. 54, issue 2, 2013, pp. 1161–1173.
- H. Eldib and C. Wang, "An SMT based method for optimizing arithmetic computations in embedded software code," *International Conference on Formal Methods in Computer-Aided Design (FMCAD'13)*. Portland, OR. 2013
- K. Bian and J. Park, "Maximizing rendezvous diversity in rendezvous protocols for decentralized cognitive radio networks," *IEEE Transactions on Mobile Computing*, vol. 12, no. 7, July 2013, pp. 1294–1307.
- K. Bian, J. Park, X. Du, and X. Li, "Ecology-inspired coexistence of heterogeneous wireless networks," *2013 IEEE Global Communications Conference (GLOBECOM)*, Atlanta, USA, Dec. 2013.
- K. Gent and M. S. Hsiao, "Functional test generation at the RTL using swarm intelligence and bounded model checking," *Proceedings of the IEEE Asian Test Symposium*, November 2013.
- K. Pabbuleti, D. Mane, A. Desai, C. Albert, P. Schaumont, "SIMD Acceleration of Modular Arithmetic on Contemporary Embedded Platforms," *2013 IEEE High Performance Extreme Computing Conference (HPEC'13)*, Waltham, MA, September 2013.
- K. Adhikari, J. Street, C. Wang, Y. Liu and S. Zhang, "Verifying a quantitative relaxation of linearizability via refinement," *International SPIN Symposium on Model Checking of Software (SPIN'13)*. Stony Brook, NY. 2013.

- L. (Nathan) Li and C. Wang, "Dynamic analysis and debugging of binary code for security applications," *International Conference on Runtime Verification (RV'13)*. Rennes, France. 2013.
- L. Zhang, A. Chattopadhyay, and C. Wang, "Round-Up: Runtime checking quasi linearizability of concurrent data structures," *IEEE/ACM International Conference on Automated Software Engineering (ASE'13)*. Palo Alto, CA. 2013.
- M. Elbayoumi, M. S. Hsiao and M. Elnainay, “Selecting critical implications with set-covering formulation for SAT-based bounded model checking,” in *Proceedings of the IEEE International Conference on Computer Design*, October 2013.
- S. Prabhu and M. S. Hsiao, *"*Test generation for circuits with embedded memories using SMT*,"* in *Proceedings of the IEEE European Test Symposium*, May 2013.
- M. Elbayoumi, M. S. Hsiao, and M. ElNainay, “Set-cover-based critical implications selection to improve SAT-based bounded model checking,” (poster) in *the IEEE/ACM Great Lakes Symposium on VLSI*, May 2013.
- M. El-bayoumi, M. S. Hsiao, and M. ElNainay, *"*A novel concurrent cache-friendly binary decision diagram construction for multi-core platforms,*"* in *Proceedings of the IEEE Design Automation and Test in Europe Conference*, March, 2013.
- M. S. Hsiao, L. Nazhandali, C. Wang, and P. Schaumont, “Counterfeit-Proof + Anti-Tamper Countermeasures = Trusted Supply Chain,” in *Government Microcircuit Applications \& Critical Technology Conf. (GOMACTech)*, Mar. 2013.
- M. Srivastav, Y. Zuo, X, Guo, L. Nazhandali, and P. Schaumont, “Study of ASIC technology impact factors on performance evaluation of SHA-3 candidates”, *Proceedings of the IEEE/ACM Great Lakes Symposium on VLSI*, May 2013.
- M. Taha, P. Schaumont, "Side-channel Analysis of MAC-Keccak",*IEEE International Symposium on Hardware-Oriented Security and Trust (HOST 2013)*, Austin, TX, June 2013.
- M. Taha, P.Schaumont, "Differential Power Analysis of MAC-Keccak at Any Key-Length," *8th International Workshop on Security (IWSEC2013)*, Okinawa, Japan, November 2013.
- M. Kusano and C. Wang, "CCmutator: A mutation generator for concurrency constructs in multithreaded C/C++ applications," *IEEE/ACM International Conference on Automated Software Engineering (ASE'13)*. Palo Alto, CA. 2013.
- P. Schaumont, "Teaching Cyber-physical Systems in Layers", *First Workshop on Cyber-Physical Systems Education (CPS-Ed 2013)*, Philadelphia, PA, April 2013.
- P. Schaumont, A. Aysu, "Three Design Dimensions of Secure Embedded Systems," *Third International Conference on Security, Privacy, and Applied Cryptography Engineering (SPACE 2013)*, October 2013, Kharagpur, India (invited paper).

- P. Schaumont, I. Verbauwhede, "The Exponential Impact of Creativity on Computer-Engineering Education", *International Conference on Micro-Electronic Systems Education 2013*, Austin, TX, June 2013.
- R. Moudgil, D. Ganta, L. Nazhandali, M. S. Hsiao, C. Wang, and S. Hall, "A novel statistical and circuit-based technique for counterfeit detection in ICs," in *Proceedings of the IEEE/ACM Great Lakes Symposium on VLSI*, May 2013.
- T. Wang and Y. Yang, "Analysis on Perfect Location Spoofing Attacks Using Beamforming," *IEEE Infocom 2013*.
- V. Kumar, J. Park, T. C. Clancy, and K. Bian, "PHY-Layer authentication by introducing controlled inter symbol interference," *IEEE Conference on Communications and Network Security (CNS)*, Washington, D.C., Oct., 2013.