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

Ferbuary 2013▪ No.009

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 Research Day in Arlington VA - 15 March 2013

On 15 March 2013, the Center for Embedded Systems for Critical Applications is organizing a public event to present its ongoing research projects.. The theme of the symposium is **Embedded Security**. During the one-day symposium, CESCA faculty will present a review of their ongoing research projects. Several project demonstrators will be on display. In the afternoon, a series of tutorials will introduce hot topics in embedded security. The event is supported by Virginia Tech National Capital Region. Registration, which includes lunch and refreshments, is free of charge. However, due to limited seating, registration is required. Please visit the following link for registration and program details:

Virginia Tech's Research Center
900 N Glebe Rd, Arlington, VA

http://www.cesca.centers.vt.edu/Events/CescaResearchDay/index.html

This event is an excellent opportunity to meet the CESCA faculty, and to meet others with similar interests. By joining this event, you will learn about current R&D directions related to secure and embedded systems. The day will start with an invited talk by Dr. Charles Clancy, director of VT's Hume Center for National Security and Technology. Next, CESCA faculty will present research reviews including design methods for secure processors and ASICs, development of secure applications in wireless and pattern recognition, and design methods for the verification of hardware and software. During lunch, participants will be able to visit demonstration booths that showcase CESCA's know-how and hands-on experience in embedded security. Company participants will be able to introduce themselves to CESCA students in Blacksburg during a video-conferencing meet-and-greet. In the afternoon, there will be four tutorials, organized as two concurrent sessions. The tutorial topics include an introduction to side-channel analysis and an introduction to Physically Unclonable Functions. There is also a tutorial on software testing and verification, and on wireless security.

The intended audience for this research day includes designers and managers from industry, government organizations, and research labs. By meeting the CESCA faculty, you will also learn about the opportunities for student recruitment, joint projects, guest seminars, and much more. We look forward in meeting you there!

CESCA Research Day Program Schedule

8:00	Registration, VT Research Center Arlington	
	Opening Session (Ballston Room)	
8:30	*Welcoming Remarks* Dr. Patrick Schaumont (CESCA Director)	
8:40	*Research Directions in Security* Dr. Charles Clancy (Hume Center Director)	
	Research Session 1: Secure Design (Ballston Room)	
9:20	*Secure ASIC Design* Dr. Leyla Nazhandali (Associate Professor, ECE)	
9:40	*Designing Secure Processors with Hardware Security* Dr. Patrick Schaumont (Associate Professor, ECE)	
10:00	Break	
	Research Session 2: Secure Applications (Ballston Room)	
10:15	*Enforcing Spectrum Access Rules in Spectrum Sharing* Dr. Jerry Park (Associate Professor, ECE)	
10:35	*Secure Smart Antennas and Radios* Dr. Yaling Yang (Associate Processor, ECE)	
10:55	*Temporal Analysis of Fingerprint Images* Dr. Lynn Abbott (Associate Professor, ECE)	
11:15	Break	
	Research Session 3: Secure Design Methods (Ballston Room)	
11:30	*Hardware Trust and Counterfeiting* Dr. Michel Hsiao (Professor, ECE)	
11:50	*Symbolic Predicitive Analysis for Concurrent Software* Dr. Chao Wang (Associate Professor, ECE)	
12:10	Lunch and Demonstrations (Smithsonian Room) CESCA Student Meet and Greet (Ballston Room)	
	Tutorial 1 (Ballston Room)	**Tutorial 2** (Farragut West Room)
1:15	*Introduction to Side-channel Analysis* Dr. Patrick Schaumont	*Software Testing and Verification* Dr. Michael Hsiao Dr. Chao Wang
3:00	Break	
	Tutorial 3 (Farragut West Room)	**Tutorial 4** (Ballston Room)
3:15	*Introduction to Physically Unclonable Functions* Dr. Leyla Nazhandali	*Wireless Security* Dr. Jerry Park Dr. Yaling Yang
5:00	Symposium ends	

From the Director's Desk

The spring semester of 2013 is well underway, and CESCA is planning a number of exciting events. The first of these is announced on the frontpage of this newsletter. On 15 March 2013, CESCA will do a **Research Day** in Virginia Tech's Research Center (Arlington, VA). We would like to welcome our project partners, sponsors and friends for a day of presentations, demonstrations and tutorials. The Virginia Tech Research Center is a state-of-the-art research center right in the heart of the Northern Virginia business and industry hub. With the help of Virginia Tech National Capital Region (http://www.ncr.vt.edu), CESCA is able to provide free registration to the attendees of the Research Day, including lunch and catering. CESCA plans to show its best, as a way of saying thank you to the community that supports and encourages our research!

This newsletter gives you a snapshot of the activities and innovations happening in CESCA.

- One of our CESCA Faculty Members, **Michael Hsiao**, was recently promoted to IEEE Fellow, for his work on to the automatic test pattern generation of integrated circuits. IEEE Fellow is a significant achievement, and CESCA is honored to have him among the faculty. The newsletter includes a short article that reviews his research and career leading up to this promotion.
- The research highlights cover our work in anti-tamper research, in counter measures against perfect-location spoofing attacks, in cognitive radio spectrum allocation, and in Javascript program verification. CESCA student Mostafa Taha gives a technology backgrounder on SHA-3.
- Our seminar series continues to attract visiting faculty and industry who give interesting and insightful talks. The seminars are recorded and posted online on our Vimeo channel. CESCA faculty member **Leyla Nazhandali** looks back at the origins of the CESCA seminars and reviews recent and upcoming talks.
- CESCA has plans to establish an award to recognize our students. Exceptional scholary work will be awarded in multiple categories, including CESCA Outstanding Student, CESCA Best Presentation, and CESCA Best Poster. **Chao Wang**, CESCA Awards Chair, explains the rules.
- We've included an interview with Scott Midkiff, Virginia Tech's Vice President for Information Technology and Chief Information Officer, on the impact of information technology on future education.

I would also like to draw your attention to the CESCA Industry Affiliate Program. Our industry partners are looking to attract top talent for their mission. CESCA can help them to identify these individuals. By partnering as a CESCA Industry Affiliate Member, you will gain a priviledged relationship to CESCA faculty and students. You will have a means for direct collaboration, for consulting, for directed research, and for joint proposal writing. Turn to the next page for further details on our IAP program.

CESCA is committed to produce the best students and scholary work in the area of embedded systems design for critical applications. We are convinced that the best research and the best graduates can only be produced by collaboration, teamwork, and critical thinking. We hope you will enjoy the articles, and we look forward to meet you on March 15 in Arlington!

Patrick Schaumont
CESCA Director

CESCA's Industry Affiliate Program

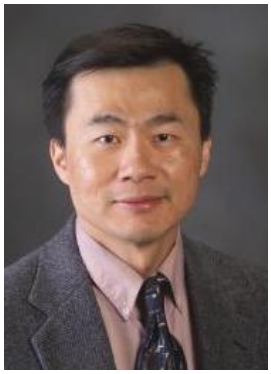
The projects carried out by CESCA Faculty and their students represent a valuable resource of intellectual property. CESCA has a model in place to help industry to benefit from this know-how and these results - CESCA's Industry Affiliate Program (IAP).

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).

Featured News

Hsiao Elevated to IEEE Fellow



CESCA would like to congratulate **Michael Hsiao**, who was elevated to IEEE Fellow, class of 2013, for his contributions to automatic test pattern generation of integrated circuits. Elevation to IEEE Fellow is an honor reserved for less than 0.1% of the voting membership of IEEE in any one year. IEEE Fellows are well recognized individuals, considered to be key contributors in the area of their specialization.

Yet, Michael remains very modest about this achievement. When asked about it, he mentioned that this honor is attributed to all those who have played a part in his academic career, starting with his Ph.D. advisor Prof. Janak Patel at the Univ. of Illinois at Urbana-Champaign, to the industrial collaborators, faculty colleagues, and the many outstanding M.S. and Ph.D. students with whom he has had the fortune to work.

Michaels' contributions to test generation are significant. Over these years, Michael has developed several test generators, with the primary applications to fault testing and design verification/validation. Additional applications of the test generators included the generation of vectors to estimate peak power, identification and locating of malicious Trojans in a circuit, high-level test generation for hardware and software, and more.

Over the years, his research has been recognized with the Best Paper Award at the 2010 Asian Test Symposium, selection among the Most Influential Papers in the First 10 Years of Design Automation and Test Conference, the NSF CAREER Award, and Virginia Tech College of Engineering Dean's Faculty Fellow. CESCA Faculty have an inspiring academic role for CESCA students and their colleagues. Elevation to IEEE Fellow is an important honor that reflects the long-term pursuit of research excellence. We wish Michael the very best in his research, and we are thrilled to have him among us!

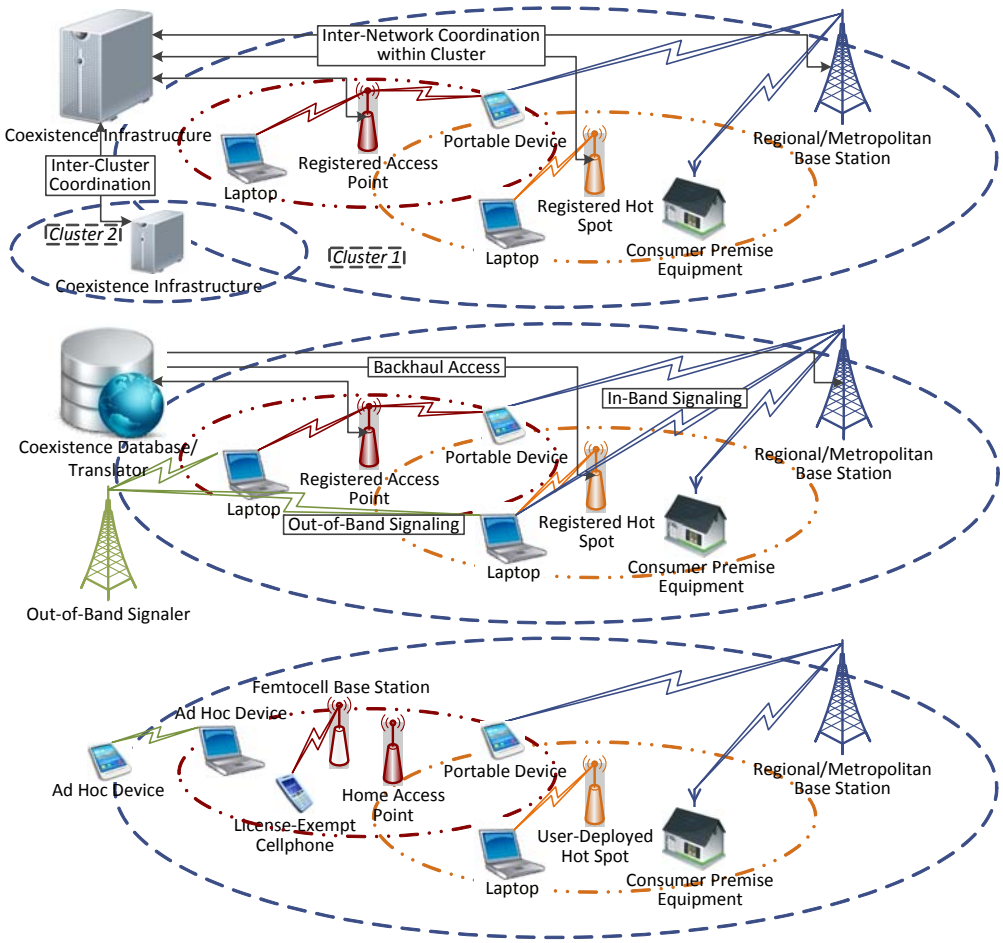
Bowyer to Deliver Keynote Presentation at CESCA Day

The 4th annual CESCA Day will be held this year on Saturday, April 20, on the Virginia Tech campus. The day will consist of research presentations, poster sessions, and other events. The keynote address will be provided by Kevin Bowyer, Department Chair of Computer Science & Engineering at the University of Notre Dame. In addition to his administrative duties, Bowyer is a well-known researcher in computer vision, biometrics, and data mining. Bowyer was named a Fellow of the IEEE for "contributions to algorithms for recognizing objects in images." He is the author of *Ethics and Computing: Living Responsibly in A Computerized World*. He is a founding General Chair of the IEEE Biometrics Theory Applications and Systems conference series, and a past Editor-in-Chief of the *IEEE Transactions on Pattern Analysis and Machine Intelligence* and of the *IEEE Biometrics Compendium*. He is also a Fellow of the International Association for Pattern Recognition and a Golden Core member of the IEEE Computer Society.

Research Highlights

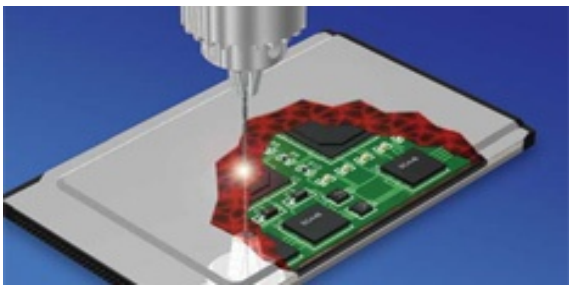
Coexistence of Cognitive Radio Networks Operating in TV White Space

With the development of dynamic spectrum access technologies, such as cognitive radio (CR), the secondary use of under-utilized TV broadcast spectrum has become a step closer to reality. Recently, a number of wireless standards that incorporate CR technology have been finalized or are being developed to standardize systems that will coexist in the same TV white space (TVWS). In these wireless standards, the widely-studied problem of primary-secondary network coexistence has been addressed by the use of incumbent geolocation databases augmented with spectrum sensing techniques. However, the challenging problem of secondary-secondary coexistence—in particular, heterogeneous secondary coexistence—has garnered much less attention in the standards and related literature. The coexistence of heterogeneous secondary networks poses challenging problems due to a number of factors, including the disparity of PHY/MAC strategies of the coexisting systems. CESCA faculty members, Drs. **Jerry Park** and **Yaling Yang**, and CESCA student, **Bo Gao**, have been studying mechanisms for heterogeneous coexistence, with a particular focus on mechanisms appropriate for TVWS. Through this research, the researchers aim is to offer a clear picture of the heterogeneous coexistence issues and related technical challenges, and shed light on the possible solution space.



Examples of heterogeneous coexistence scenarios: a) centralized mechanisms (top), b) coordinated mechanisms (middle), and c) autonomous mechanisms (bottom).

CESCA Faculty Collaborate on Anti-tamper Research

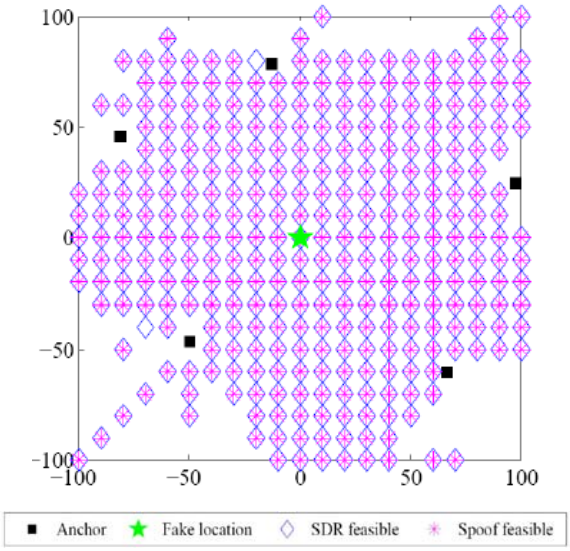


CESCA faculty members, **Michael Hsiao**, **Leyla Nazhandali**, **Chao Wang** and CESCA student **Avinash Desai**, are collaborating on a research project on trusted hardware and have presented a new way to protect against tampering by a clever obfuscation of the design, which can be unlocked with a specific, yet dynamic path traversal in the circuit. Hence, the functional mode of the controller is hidden with the help of obfuscated states, and the functional mode is made operational only on the formation of a specific interlocked Code-Word logic during state transition. No comparator is needed to check as the obfuscation is embedded within the transition function of the state machine itself. A side benefit is that any small alteration will be magnified via the obfuscated design. In other words, an alteration to the design will manifest itself as a large difference in the circuit's functionality.

A New Project on JavaScript/Web Program Verification

What's the *Programming Language of the Web*? Your guess is correct – JavaScript is the de facto language for programming in web browsers, to control browser behavior such as open a menu, show a pop-up, or get information back from the server. Well written JavaScript programs are important for ensuring the security and privacy of client side applications. However, the highly dynamic nature of this language -- for instance, it's weakly typed and allows classes and functions to be declared on the fly – poses severe challenges to testing and verification. Dr. **Chao Wang**'s group recently started a project on JavaScript/Web program verification, with support from Fujitsu Laboratories of America (FLA). They are developing new methods that combine both static analysis and symbolic execution to improve the precision and scalability of the verification procedure. Dr. Wang's Ph.D. student, **Lu Zhang**, is currently working as a research intern at Fujitsu Labs.

Yang identifies countermeasures against Perfect Location Spoofing Attacks



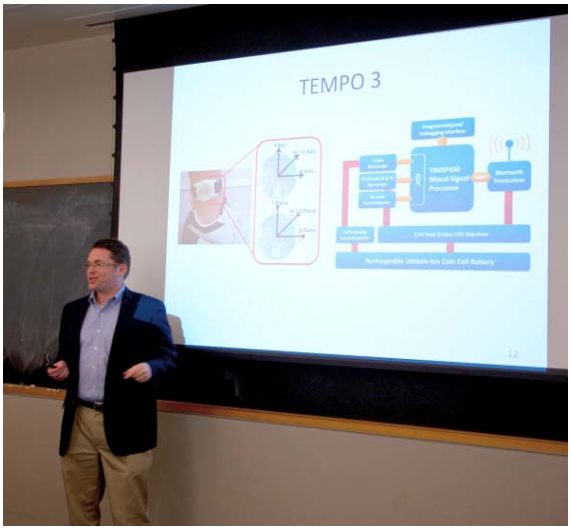
Radio localization systems have been integrated into many wireless network solutions. For example, location-based access control determines the users' privileges of accessing critical information by taking the users' physical locations into account. Identity spoofing detection mechanisms use location information to differentiate malicious nodes from legitimate nodes. In these applications, the correctness of the location results provided by the localization systems is critical. Attacks on localization systems can cause errors in location estimation and consequently break these location based mechanisms of wireless networks. Many efforts have been put into the detection of location spoofing attacks through detecting the abnormality in radio's signal features. However, despite all the existing efforts, we have discovered that these existing schemes are all limited in their effectiveness. In many circumstances, there exist location-spoofing attacks that can stay undetected under all of these robust localization algorithms. Such attack is called a "*perfect location spoofing (PLS) attack*". CESCA faculty member **Yaling Yang** and CESCA student **Ting Wang** built a theoretical model to analyze the feasibility of PLS attacks and how it is affected by the localization anchor deployment. Specifically, she formulated PLS as a nonlinear feasibility problem based on smart antenna array pattern synthesis. The intractable nature of this feasibility problem requires a solution using semidefinite relaxation (SDR) in conjunction with a heuristic local search algorithm. This analytical approach can provide insightful advices for spoof-resistant localization anchor deployment, so that the threat of PLS attacks can be minimized.

CESCA Training and Seminars

CESCA Faculty to Deliver Biometrics Training

CESCA faculty members **Lynn Abbott** and **Michael Hsiao** are part of a team that is providing a series of training modules to the Biometrics Support Center, which is a unit of the US Department of Homeland Security. **Abbott** and **Hsiao** will present an overview of biometrics, to include physiological biometrics such as fingerprint and iris modalities, as well as behavioral biometrics such as keystroke recognition. Other team members include **Kathleen Meehan** of the Electrical Engineering Department, **Edward Fox** of the Computer Science Deparment, and **Eric Smith** of the Statistics Department.

Origins of the CESCA Seminar Series



Prof. John Lach (UVA) presenting the CESCA seminar (2/8/13)

CESCA has had a great tradition of seminar presentations, which dates back to 2007. The goal of the CESCA seminar program is to establish a friendly research culture that allows the CESCA students and faculty interact with distinguished speakers on the topics of interest related to CESCA. Our esteemed speakers are invited from various universities, companies and national research labs. Since CESCA, as a center, attempts to address the major challenges in the conception, design, and implementation of next-generation embedded systems, the topics of our weekly seminars cover a wide range of subjects related to embedded systems. These include advanced topics in networking, embedded systems hardware and software design, specific embedded applications, etc. In 2012, CESCA held 17 seminars throughout the year. All CESCA seminars are videotaped and are publicly available on CESCA website.

http://www.cesca.centers.vt.edu/Events/PreviousSeminars/index.html

CESCA Seminars in Spring 2013

- Neil Steiner (University of Southern California, ISI), "TORC: Open-Source Tools for Reconfigurable Computing"
- John Lach (University of Virginia), "Body Sensor Networks: An Application-centric Approach"
- **Upcoming 3/1/13**: Salaam Houman (George Mason University), "Dynamically Heterogeneous COres through 3D Resource Pooling"
- ***Upcoming 3/22/13***: Ravi Tandon (VT)
- ***Upcoming 3/29/13***: Ali Butt (VT)
- ***Upcoming 4/26/13***: Romit Choudhury (Duke University)
- ***Upcoming 5/3/13***: Dangfeng Yao (VT)

In spring 2013, CESCA Seminars are held on
Fridays, 2:30PM - 3:15PM, Lavery Hall 330

CESCA Seminars in Fall 2012

- Pamela Abshire (University of Maryland), "BioChips: Learning from Biology"
- Gabe Westmaas (Rackspace), "Learning to Scale a Public Cloud"
- Linda Xie (University of North Carolina Charlotte), "Distributed Broadcast in Multi-hop Cognitive Radio Networks"
- Nathan Li (Battelle Memorial Institute), "The Chronicles of Cyber Security: The offense, the defense and the analytics"
- Wuchun Feng (VT), "An Ecosystem for the New HPC: Heterogeneous Parallel Computing"
- Amira Youssef (ITI Alexandria, Egypt), "Image Watermarking Techniques using Histogram Tailored Chaotic Maps"
- Carlos A. Gonzalez (Power Fingerprinting), "Power Fingerprinting for Integrity Assessment of Critical Embedded Systems"
- Jonathan Graf (Luna Innovations Inc), "FPGA Trust - Ensuring Design Integrity through Analysis of FPGA Bitstreams and IP Cores"

Technology Backgrounder

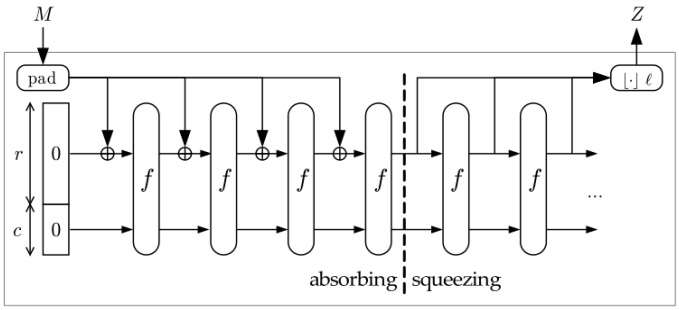
The Birth of a New Hashing Standard: SHA-3

by Mostafa Taha

A cryptographic hash function converts an arbitrary-length message into a fixed-length digest, and it is a fundamental step in the efficient implementation of electronic messages. Back in 2004, significant attacks on the standard hash functions of that time were getting published everywhere. These attacks almost completely broke MD5, SHA-0 and later on SHA-1. At that time, NIST announced to phase out SHA-1 and replace it with the more stable, SHA-2. However being algorithmically similar to SHA-1, NIST had the fear that SHA-2 might itself get broken in the near future, and announced in Nov 2007 for a competition to select a new standard for cryptographic hashing, SHA-3. Out of 64 submissions, the competition ended on Oct 2012 with Keccak as the winner. Keccak (pronounced “ketchak”) was designed by a cryptographic group from Belgium and Italy, namely Guido Bertoni, Joan Daemen, Gilles Van Assche of

STMicroelectronics and Michaël Peeters of NXP Semiconductors. Interestingly, Joan Daemen is also a co-author of the block cipher Rijndael who won the AES competition. Later research on the cryptanalysis of hashing algorithms improved the confidence in SHA-2 showing that it can still be safely used. This conclusion slightly encouraged NIST to favor Keccak for being an entirely different algorithm. "It seems very unlikely that a single new cryptanalytic attack or approach could threaten both algorithms," as quoted from the NIST announcement statement. Currently, it appears that NIST will keep the two algorithms as a backup for each other.

Keccak uses a new *Sponge Construction* chaining mode with a fixed permutation function (*f*) as shown in the figure. The idea is to limit the effect of the new input data to only *r* (rate) bits of the internal state. The rest of the state, of size *c* (capacity) is not directly affected by the current input. The capacity is used as a design parameter to trade security strength for throughput. The size of the internal state of Keccak is 1600 bits organized as a 5×5×64 array, with the rate and capacity configured according to the desired level of security. The Keccak SHA-3 standard proposes digest of 224, 256, 384 and 512 bits. The permutation function is simple yet effective, resulting in Keccak's remarkable performance in hardware modules (ASICs and FPGAs). The designers augmented Keccak with different modes of operation to extend its use toward authentication, random number generation, and high-performance parallel implementation.



The Sponge Construction, from http://sponge.noekeon.org/

CESCA has contributed to the selection process by supporting the hardware benchmarking of the candidates. Under a NIST funded project lead by CESCA faculty members **Patrick Schaumont** and **Leyla Nazhand-Ali**, we designed an ASIC chip with all the final round algorithms and provided their performance results. We shipped the SHA-3 ASIC to 8 different research groups all over the world for various performance and security evaluations. The project still continues with evaluating the vulnerabilities of the winner algorithm 'Keccak' against different types of Implementation Attacks.

CESCA Establishes CESCA Student Awards

The CESCA faculty members have established new awards to be given each year to students who have made the most significant contributions to the research, education, and service activities of CESCA. There are four categories of student awards: CESCA Outstanding Student Awards, CESCA Best Presentation Awards, CESCA Day Best Poster Awards, and CESCA Outstanding Service Awards. The candidates will be nominated and selected by the CESCA faculty members during the spring semesters. We will honor the awardees during our annual CESCA Day event in April. For more information, please contact Dr. **Chao Wang**, who is serving as the CESCA Awards Chair for the academic year of 2012-2013. The detailed selection criteria are listed as follows:

CESCA Outstanding Student Award: Students who have published five or more first-author papers in top journals or peer-reviewed conferences will be eligible for competing for this award. Each student can receive this award at most once. However, there may be more than one recipient per year.

CESCA Best Presentation Award: Students who have published a journal or top-tier conference paper in that year will be eligible for competing for this award. The winner -- one per year -- will be decided jointly by the CESCA faculty members. Please consult the advisor for a list of conferences in your area.
CESCA Day Best Poster Award: Students who participate in the poster sessions during our annual CESCA Day event will be eligible for competing for this award. The winner -- one per year -- will be decided jointly by the CESCA faculty members.
CESCA Outstanding Service Award: Students who have made significant contributions to improving the academic, research, educational, and social environment of CESCA will be eligible for competing for this award. The recipient -- one per year -- will be decided jointly by the CESCA faculty members.

CESCA Interview - Scott Midkiff

As ECE Department head, Scott Midkiff hired our most recent CESCA Faculty member. Recently, he became Virginia Tech's Vice President for Information Technology and Chief Information Officer. CESCA visited Scott to talk about IT, and its impact on education and research.

CESCA: Could you tell a bit about your earlier appointments, and how that evolved into your current position?

Midkiff: I came to Virginia Tech in 1986 as an assistant professor and progressed through the faculty ranks. My Ph.D. research had been at the intersection of VLSI design, parallel computing, and networking. I had also done some research in VLSI testing. Over time, my research adapted to focus more on networking and then on mobile and wireless networks, as well as how to use networks for multimedia applications and pervasive computing. To some extent, my research has been hampered by being broad, but I have always liked to look at problems in context and to be driven by applications. Narrow, deep research and broader, systems research are both important to advancing knowledge and technology. But, I have always been in the “broad” and “systems” camps.

I have also always enjoyed working with people. First and foremost, I have always found working with students to be very rewarding. I have learned much from students and I hope they have learned from me. My most important contributions as a professor are the students I have taught and the masters and Ph.D. students that I have advised. I have always tried to integrate research and education with this in mind. I have also sought out collaborations with colleagues in Electrical and Computer Engineering and in many other departments.

My interests in looking at research broadly, working with people, and continuously learning led me to spend 2006 to 2009 as a program director at the National Science Foundation. I had wonderful opportunities at the NSF to help create and run the Cyber-Physical Systems program; initiate the “cyber” mission of the Electrical, Communications and Cyber Systems Division; contribute to the Integrative Graduate Engineering and Research Training program for which I had earlier been a principal investigator; and to contribute to cyberinfrastructure programs both within the Directorate for Engineering and at the Foundation level.

From 2009 to 2012 I had the great honor of serving as the department head for ECE. As an NSF program director and as a department head, my primary focus changed from my research and teaching to serving the research community at the NSF and to serving ECE students, faculty, and staff as department head. Serving as an NSF program director exposed

me to many different researchers from different institutions. As ECE department head, I learned more about our ECE department and other ECE departments across the country, the College of Engineering, and the University.

I was enjoying my term as ECE department head and was looking forward to continuing and beginning initiatives in the department when I was presented with the opportunity to serve as Virginia Tech's Vice President for Information Technology and Chief Information Officer. This position offers me the opportunity to leverage technical expertise, teaching and research experience, and knowledge of Virginia Tech to lead a fantastic IT organization that serves students, faculty, and staff across the university. Information technology has never been more important to teaching and learning, research, and the operation of the university. I am honored to have the opportunity and the challenge to serve and to lead at such an important time and in such an important function for Virginia Tech.

CESCA: What are your tasks as Virginia Tech's Vice President for Information Technology and Chief Information Officer?

Midkiff: The Information Technology organization at Virginia Tech has broad responsibilities. We strive to provide leading-edge computing and networking infrastructure, ensure that Virginia Tech effectively leverages IT for teaching and learning, enable advanced research computing and visualization, support and advance enterprise systems to aid the effective operation of the university, secure the university's IT infrastructure and data, contribute to the safety and security of the university community, and build partnerships and collaborations within and beyond Virginia Tech consistent with university goals. For faculty and students, our most "visible" components include email, identity management and secure login, the wired and wireless network and Internet connectivity, Scholar, emergency message boards, and the telephone system. Information technology services are provided by many organizations on campus, such as by the IT staff in the ECE department and by students in CESCA. "Central IT" provides services that need university-level scale for effectiveness. Increasingly, we act as brokers for services like Google Mail where even higher levels of scale are advantageous. An essential part of our mission is to innovate. We focus on those services where there are opportunities to innovate and improve or to otherwise provide an advantage to the university.

While I am ultimately responsible for the operational aspects of IT, we have a great team and set of line managers that make things work. My goal as VPIT and CIO is to integrate across the current and, especially, future needs of the university; the capabilities of the IT organization and what those capabilities should be; and the changing landscapes of technology and higher education to ensure that Virginia Tech is positioned for the future as a leader in education, research, and outreach.

CESCA: Do you think information technology will fundamentally change how students learn?

Midkiff: There are (at least) two ways to think about this, how students learn as a cognitive process and how students are educated and earn degrees.

With respect to how students learn as a cognitive process, information technology will not so much fundamentally change how students learn as it will allow students to learn in a manner that is best for them. Education researchers have long recognized different learning styles. For example, learners can be, to varying degrees, active or reflective, sensing or intuitive, visual or verbal, and sequential or global. As faculty, we tend to teach for one particular style of learning which may not be the best for many or even most of our students. With appropriate use of technology, students can access and process concepts in different ways according to their individual learning styles. Already, some instructors are using technology with techniques such as "flipping the classroom" to restructure how they spend their

time with students and what students do outside of class. In the distant future, more radical and truly fundamental changes may be possible, such as using brain science to customize and adapt learning stimuli.

Information technology may also change how students are educated and earn degrees. This is at the heart of the buzz around massively online open courses, or MOOCs. There is the hope that students will have the opportunity to learn at anytime, anywhere, and from anyone at a very low cost given economies of scale. I believe we can learn a lot from MOOCs, but there are still open questions regarding assessment, quality control, and support for different learning styles. Virginia Tech has been active in online distance learning for more than 12 years. An example is the Master of Information Technology program to which ECE contributes. Our challenge now is to use that experience as well as technological and other advances to improve learning for all of our students, both locally and at a distance, and to develop more flexible and efficient ways to teach and learn. Also, I also believe that "place" is extremely important for students that come to Virginia Tech and many other universities. We need to ensure that our campus is differentiated through information technology in how it supports learning, in the classroom and beyond.

CESCA: Modern information technology seems to evolve as a symbiosis of embedded devices on the one hand, and big-data cloud computing on the other hand. How will this affect Virginia Tech?

Midkiff: This topic is on the minds of many university CIOs. The "consumerization" of IT allows students, faculty, and staff to bring increasingly advanced and diverse types of devices to campus. This is referred to as the bring-your-own-device, or BYOD, phenomena. And, fast networks and economies of scale make "the cloud" increasingly attractive for many services. As an IT organization, we need to let people be productive with their devices and we need to ensure that the university leverages the capabilities and efficiencies of cloud computing. This will push IT to serve more often as a consultant and as a broker. And, of course, we need to be concerned about security and privacy in all of this.

Services that are commodities – where we see little need or opportunity for innovation and improvement – are good targets for the cloud. Also, high-performance computing in the cloud might serve the needs of researchers able to do their work on a highly abstracted computing platform. In addition, HPC in the cloud might allow the university to offer near limitless numbers of processor nodes to investigators, with most demand being met with fast, lower cost local resources and infrequent peak demand being met by cloud services at a higher marginal cost.

It is interesting that the "Internet of Things," which is sort of the cloud of embedded systems, is on campus today, albeit in simple forms. We have Internet-connected soft drink machines, door locks, parking lot gates, message boards, and cameras. This trend will only grow as embedded systems advance. And, I believe we will see more pervasive computing services for learning and research, such as technology-rich spaces for group learning and collaboration.

CESCA: Computer engineers face an ever faster pace of innovation, and technological knowledge seems to have a shrinking shelf life. How can we prepare our students to survive in the information technology age? Should they specialize or diversify?

Midkiff: This is a challenging issue. By being very specialized, one's knowledge can quickly become irrelevant due to innovation and technological change. Diverse knowledge is good, but the complexity of many of today's technologies makes it difficult to have a sufficiently deep understanding of more than a single technology. Today's students need to develop several capabilities to prosper as engineers in the future. These are not necessarily new capabilities,

but they are increasingly important for not only success, but for basic competency. When I was a fresh graduate working as an engineer, before the Internet was pervasive and before the World Wide Web had been developed, engineers had to have lots of information and procedures at the ready. Today we have access to too much information. Engineers need to be able to filter, process, and integrate information. Systems and systems of systems are increasingly important. An ability to think at a systems level and at different levels of abstraction is essential to keep pace with the ever increasing complexity of technology. While a dissertation topic may be very focused, it is important to think about the work in the context of a system. The ability to effectively process and integrate information and systems thinking are abilities that maintain value even as technology changes. And, engineers must learn to continuously adapt and embrace change. It's great that we are in a profession where we can always learn, always be challenged, and always have an opportunity to change the world.

The pace of innovation is just one of several challenges that will face engineers and engineering educators in the coming years. If they have not already done so, faculty members and students interested their futures should read *Educating the Engineer of 2020: Adapting Engineering Education to the New Century* (National Academies Press, 2005).

CESCA: If you think about the information systems of the future, do you think there are fundamental technological limits (like Moore's law) that will hold us back? Or, is the only limit our imagination?

Midkiff: If we think about what we wish to achieve, rather than how to achieve it, I really do think we are limited only by our imaginations and our willingness to invest in making imagination become reality. I recall a seminar I attended as an undergraduate in 1979 where the theme was that we were approaching the limits of semiconductor technology and that parallelism was the only way to improve computing performance. In the 34 years since then, we have gone from processors with about 29 thousand transistors (the Intel 8086 of 1978) to about 5 billion transistors (the Intel 62-core Xeon Phi of 2012). Of course, multicore processors like the Xeon Phi do use parallelism, but this is driven by design complexity and architectural tradeoffs given clock speed limits, and not by limited transistor counts due to some demise of Moore's Law. In my opinion, complexity will continue to be the biggest barrier to advancing the capabilities of information systems of the future. But, I am confident that we will find clever architectures, new computing components, and new design methods to deal with this complexity.

CESCA: Thank you very much for sharing your insights. We wish you best of luck in your position as Vice President and CIO!

Student News & Highlights

Recent Graduations

- Min Li (advisor: Hsiao), Ph.D., Dissertation Title: "Acceleration of hardware testing and validation algorithms using graphics processing units". Joined Google.
- Gyanendra Shrestha (advisor: Hsiao), M.S., Thesis Title: "Ensuring trust of third-party hardware design with constrained sequential equivalence checking". Joined NVidia.
- Nathan Short (advisor: Abbott), Ph.D., Dissertation Title: "Robust Feature Extraction and Temporal Analysis for Partial Fingerprint Identification". Joined Booz Allen.
- Lyndon Judge (advisor: Schaumont), M.S., Thesis Title: "Design Methods for Cryptanalysis". Joined Intel.

New CESCA Students Fall 2012

- Aydin Aysu, PhD student (Advisor: Schaumont)
- Kiran Adhikari, MS student (Advisor: Wang)
- Arijit Chattopadhyay, MS student (Advisor: Wang)
- Nahid Farhady Ghalaty, PhD student (Advisor: Schaumont)
- Seungmo Kim, PhD student (Advisor: Park)
- Deepak Mane, MS student (Advisor: Schaumont)
- Vineeth Acharya, MS student (Advisor: Hsiao)
- Sharad Bagri, MS student (Advisor: Hsiao)
- Krishna Pabbuleti, MS student (Advisor: Schaumont)

Publications

- D. Bakshi and M. S. Hsiao, “LFSR seed computation and reduction using SMT-based fault-chaining,” to appear in Proceedings of the IEEE Design Automation and Test in Europe Conference, March, 2013.
- M. El-bayoumi, M. S. Hsiao and M. ElNainay, “A novel concurrent cache-friendly binary decision diagram construction for multi-core platforms,” to appear in Proceedings of the IEEE Design Automation and Test in Europe Conference, March, 2013.
- A. Desai, M. S. Hsiao, C. Wang, L. Nazhandali, and S. Hall, "Interlocking obfuscation for anti-tamper hardware," in Cyber Security and Information Intelligence Research Workshop, Jan. 2013.
- S. Wu, L.-T. Wang, X. Wen, W.-B. Jone, M. S. Hsiao, F. Li, J. C.-M. Li, J.-L. Huang, "Launch-on-shift test generation for testing scan designs containing synchronous and asynchronous clock domains," in ACM Trans. Design Automation of Electronic Systems, vol. 17, no. 4, 2012.
- H. Nguyen and M. S. Hsiao, "Sequential equivalence checking of hard instances with targeted inductive invariants and efficient filtering strategies," in Proceedings of the IEEE High Level Design Validation and Test Workshop, November 2012.
- M. Li, K. Gent, and M. S. Hsiao, "Design validation of RTL circuits using evolutionary swarm intelligence," in Proceedings of the IEEE International Test Conference, November, 2012.
- G. Shrestha and M. 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.
- D. Bakshi, S. Prabhu, and M. S. Hsiao, "LBIST Reseeding With a New SMT-based Chainability Analysis," in SRC TECHCON, September 2012.
- 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, vol. 54, issue 2, 2013, pp. 1161–1173.
- B. Bahrak and J. Park, “Security of spectrum learning in cognitive radios,” SK Telecom Telecommunications Review, vol. 22, no. 6, Dec. 2012, pp. 850–864.
- N. J. Short, A. L. Abbott, M. S. Hsiao, and E. A. Fox, “Temporal Analysis of Fingerprint Impressions,” *Proceedings: IEEE Fifth International Conference on Biometrics: Theory, Applications and Systems* (BTAS 2012), Arlington, VA, Sept. 2012.
- N. J. Short, A. L. Abbott, M. S. Hsiao, and E. A. Fox, “Robust Feature Extraction in Fingerprint Images using Ridge Model Tracking,” *Proceedings: IEEE Fifth International Conference on Biometrics: Theory, Applications and Systems* (BTAS 2012), Arlington, VA, Sept. 2012. (Runner-up for Best Student Paper award.)

- P. Schaumont, “A Practical Introduction to Hardware/Software Codesign - 2nd Edition,” Springer Circuits and Systems Series, (xviii + 480 pages), ISBN 978-1-4614-3736-9, Springer 2013.
- Z. Chen, A. Sinha, P. Schaumont "Using Virtual Secure Circuit to Protect Embedded Software from Side-Channel Attacks", IEEE Trans. Computers, 62(1): 124-136 (2013).
- L. Judge, M. Cantrell, C. Kendir, P. Schaumont, "A Modular Testing Environment for Implementation Attacks," Workshop on Redefining and Integrating Security Engineering at ASE/IEEE International Conference on Cyber Security 12 (RISE), December 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.
- M. Taha, P. Schaumont, "A Novel Profiled Attack in the Presence of High Algorithmic Noise," International Conference on Computer Design (ICCD 2012), September 2012.
- L. Judge, S.Mane, P. Schaumont, "A Hardware Accelerated ECDLP with High-performance Modular Multiplication," International Journal of Reconfigurable Computing (IJRC), Hindawi Publishers, September 2012.