Center for Embedded Systems for Critical Applications

VirginiaTech
Invent the Future

CESCA Newsletter
Center for Embedded Systems for Critical Applications

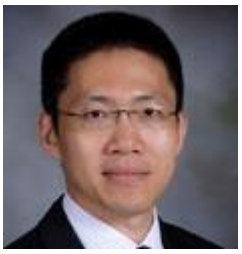
CESCA • 302 Whittemore Hall • Dept. of ECE • Virginia Tech • Blacksburg • 24061 • USA

April 2014▪ No.011

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

FMCAD 2013 Best Paper Award



Chao Wang

Hassan Eldib

Dr. Chao Wang and his Ph.D. student, **Hassan Eldib**, received the Best Paper Award at the International Conference on Formal Methods in Computer Aided Design (FMCAD) in November 2013 for a paper titled "An SMT based method for optimizing arithmetic computations in embedded software code." FMCAD 2013 is a leading conference on the theory and applications of formal methods in hardware and system verification, providing a forum to researchers in academia and industry for presenting and discussing groundbreaking methods, technologies, theoretical results, and tools for reasoning formally about computing systems. According to the FMCAD 2013 Best Paper Committee, Eldib and Wang's work "tackles a very interesting problem, namely the optimization of control software manipulating fixed-point integer data, and presents an innovative and scalable solution based on the use of SMT solvers and inductive synthesis procedures" and is "an important step towards the design of better embedded software."

DySPAN 2014 Best Paper Award

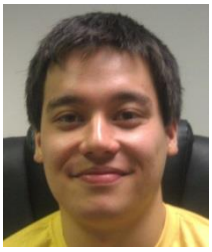
Members of **Dr. Jerry Park**'s research group along with others were recently awarded a **Best Paper Award** at the 2014 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN) conference. IEEE DySPAN is the premier conference to discuss, publish, and present recent advancements in Dynamic Spectrum Access (DSA) and Cognitive Radio, including novel approaches and technologies enabling more efficient use of the radio spectrum. Full citation of the paper is: B. Bahrak, S. Bhattarai, A. Ullah, J. Park, J. Reed, and D. Gurney, "Protecting the primary users' operational privacy in spectrum sharing," IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), April 2014.

ICDP-13 Best Poster Award

Members of **Dr. Lynn Abbott**'s research group attended the 5th International Conference on Imaging for Crime Prevention and Detection (ICDP-13) in December, 2013, and received the

Best Poster Award for their work involving the analysis of handwriting. Visiting Scholar **Dr. Amira Youssef** and Ph.D. student **Ahmed Ibrahim** worked with Dr. Abbott to coauthor the paper "Automated Gender Identification for Arabic and English Handwriting." This conference brings together researchers, industry representatives, and end users, including law-enforcement officers. Attendees share experiences and explore areas where additional research and better working practices are needed.

Harry Lynde Bradley Fellowship



Markus Kusano

Markus Kusano, an REU student who has been collaborating with Dr. Chao Wang in the past two years, received the prestigious Harry Lynde Bradley Fellowship from the ECE Department at Virginia Tech. It is the department's highest honor bestowed upon its graduate students. Markus has maintained an excellent academic record and been on the Dean's List throughout his undergraduate years. He published a first-author paper at the IEEE/ACM International Conference on Automated Software Engineering in 2013. His REU project also led to the release of a new open-source software tool called CCmutator on Github. The Bradley fellowship provides generous academic year support, including tuition, stipend, and fund for travel to conferences and other professional meetings, for up to three years of his Ph.D. studies. Markus plans to take advantage of the flexibility offered by this fellowship to pursue truly innovative research.

From the Director's Desk

After enduring a winter storm for every letter of the alphabet, there's no such thing as exciting as a little bit of sunshine! The academic year is whizzing forward and shortly CESCA will graduate another batch of Master's and PhD students. We wish those students the very best, and we are proud have helped them one step ahead in their career. Good luck to **Behnam Bharak** (PhD fall 2013), **Mostafa Taha** (PhD spring 2014), **Arijit Chattopadhyay** (MS spring 2014), **Deepak Mane** (MS spring 2014) and **Krishna Pabbuleti** (MS spring 2014).

CESCA is the Center for Embedded Systems for Critical Applications. A critical application, in a nutshell, is one in which failure will result in harm to its users. In this newsletter, you will find an update on the latest research activities and achievements in CESCA. But I would like to point out a few noteworthy highlights.

- CESCA Student **Hassan Eldib** and his advisor **Chao Wang** received a Best Paper Award at FMCAD 2013, a leading conference on the theory and applications of formal methods in hardware and system verification. We congratulate both of them on this important recognition.
- CESCA Students **Behnam Barak** (recently graduated), **Sudeep Battarai**, and their advisor **Jung Min "Jerry" Park** received a Best Paper Award at IEEE Dyspan 2014, an International Symposium on Dynamic Spectrum Access Networks. Likewise, visiting scholar **Dr. Amira Youssef**, Ph.D. student **Ahmed Ibrahim**, and their advisor **Lynn Abbott** received a Best Poster Award at the 5th International Conference on Imaging for Crime Prevention and Detection (ICDP-13)

- CESCA Day 2014, which will be help on 19 April 2014, will welcome Prof. Marilyn Wolf from Georgia Tech. Dr. Wolf is a leading researcher in the embedded systems design field, and has been a founding member of several of today's leading conferences in embedded system design (such as CODES/ISSS and ESWEEK). We highly anticipate her talk on CESCA Day, "A Brief History of Embedded Computing: From the Distant Past to the Far Future"!
- CESCA hosted a visit by Dr. Bob Colwell, director at the DARPA MTO office and chief architect of the Intel Pentium series.
- Team Envision, a CESCA-based group of ECE students who participate in the Cornell Cup, is ramping up to participate in the Cornell Cup final competition which will be held in Orlando in early May. A short article in this newsletter enumerates the highlights of their design.

CESCA is an exciting research environment and continuing growth. In 2013, CESCA faculty acquired $3484K in new funding, from a diverse collection of sponsors including NSF, NIH, ONR, Fujitsu, and Motorola. We also published 11 journal publications, 35 conference publications and 1 book. We also have a very active seminar series, including 17 seminars in 2013; I would like to acknowledge the efforts of Chao Wang as the seminar organizer for this year.

As a closing point, I would like to thank all CESCA faculty and student researchers for making CESCA the place it is today. I must also thank CESCA members work on CESCA's visibility: Nahid Farhady Ghalaty for working on posters for the CESCA Hallway display, Xiangwei Zheng for working on the CESCA TV Display, Akiko Nakata for keeping the CESCA website brimming and up to date, and Dr. Michael Hsiao for editing the CESCA Newsletter.

Patrick Schaumont
CESCA Director

Featured News

CESCA Day 2014 welcomes Prof. Marilyn Wolf

Prof. Marilyn Wolf

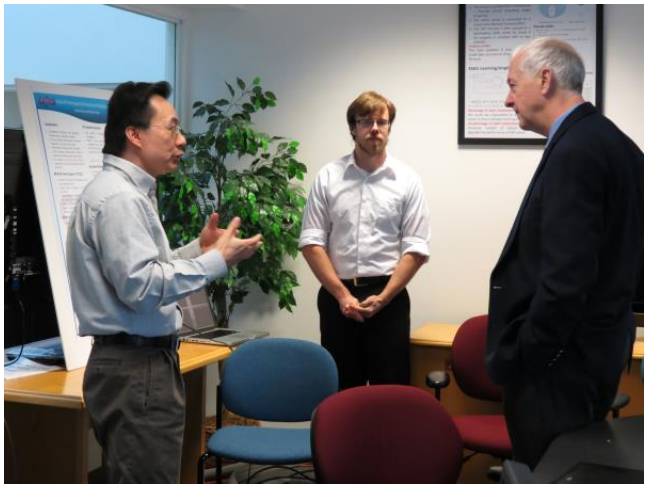
On 19 April CESCA will host Prof. Marilyn Wolf from Georgia Tech as the keynote speaker of the 5th CESCA Day. Marilyn Wolf is Farmer Distinguished Chair and Georgia Research Alliance Eminient Scholar at the Georgia Institute of Technology. She is a well-known researcher in embedded systems design, cyber-physical systems, enbedded video and computer vision, and VLSI systems. The Keynote talk is entitled "A Brief History of Embedded Computing: From the Distant Past to the Far Future".

CESCA Day 2014 will be held at Claytor Lake State Park in Dublin, VA. The day is the annual research event for CESCA. After the keynote by Dr. Wolf, students will present their latest research in poster sessions. CESCA will also recognize students with exceptional performance by handing out awards for CESCA Best Presentation, CESCA Best Poster, Outstanding CESCA Student, and CESCA Service. Full details of CESCA Day, including the program, will be available on the web (http://www.cesca.centers.vt.edu/events/cescaday/index.html)

DARPA MTO Director Bob Colwell Secure visits CESCA

On 26 February, 2014, CESCA hosted a visit by Dr. Bob Colwell, DARPA MTO Director. The full-day visit by Dr. Colwell to the ECE Department included a Bradley Distinguished Seminar entitled 'If you did not test it, it does not work'. Dr. Colwell related to his extensive experience of a career in the computer industry making exactly this point.

The CESCA Faculty presented and demonstrated their latest research efforts, including a demo on side-channel analysis and a secure sensor node (Schaumont), the SC-Sniffer compiler for side-channel resistant software (Wang), functional verification using Ant Colony Optimization (Hsiao), and facial expression recognition (Abbott). Dr. Colwell is well known for his work on the IA-32 architecture used in Intel's Pentium Pro, Pentium II, Pentium III and Pentium 4 microprocessors. He authored a book on his experience ("The Pentium Chronicles"), and he has been a recognized columnist in IEEE Computer for several years.



Bob Colwell is briefed on CESCA's research in functional verification by Michael Hsiao and PhD Candidate Kelson Gent.
See also their article in this newsletter.

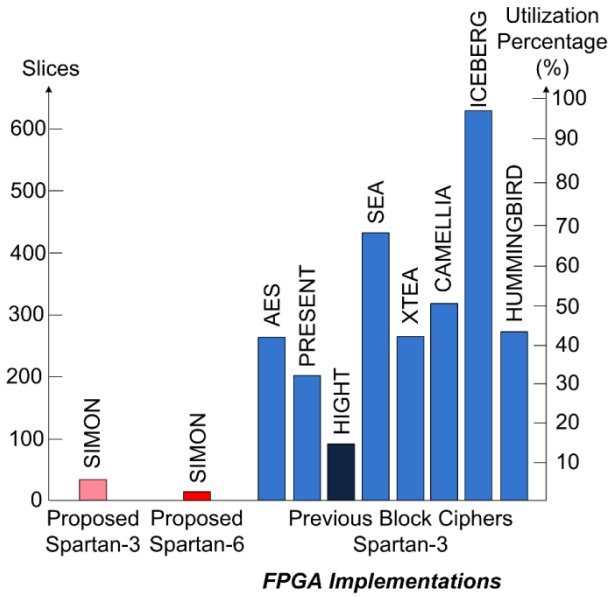
Research Highlights

Secure Embedded Systems Lab Implements the World's Smallest 128-bit Encryption Engine

In today's digital systems, we extensively use the Advanced Encryption Standard (AES) to implement security. However, the cost of AES limits its deployment in resource-constrained platforms. This lead into a new research area called the light-weight cryptography. Several light-weight alternatives of AES was introduced over the years and some have even been standardized by IEEE. Most recently, NSA has proposed SIMON, a hardware-optimized encryption algorithm which claims to be the smallest ever invented. Yet, as of now, the researchers did not know the hardware architecture that can achieve these results.

At Secure Embedded Systems lab, **Aydin Aysu**, **Ege Gulcan** and **Patrick Schaumont** shows an ultra-low-cost hardware architecture for the FPGA implementation of SIMON. Their work was accepted to be published in the upcoming issue of the IEEE Embedded Systems Letters.

The researchers first analyze the design space of the encryption engine and then propose a bit-serial, light-weight implementation. The proposed area-optimized hardware architecture is 7x smaller than AES and 3x smaller than the smallest encryption engine ever published. Therefore, it sets the new area records of symmetric key encryption on FPGAs. The group plans to extend their work by implementing an ASIC and test its security against several attack methods.



The area cost of the SIMON and previous encryption engines on FPGAs

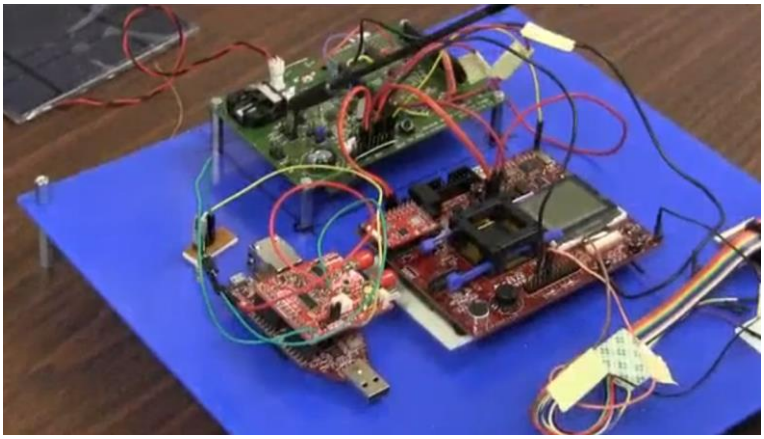
An Energy-harvesting Secure Sensor Node

The Internet of Things will include many resource-constrained wireless sensing devices, hungry for energy, bandwidth and compute cycles. The sheer amount of devices involved will require new solutions to handle issues such as identification and power provisioning. First, to simplify identity management, device identification is moving from symmetric-key solutions to public-key solutions. Second, to avoid the endless swapping of batteries, passively-powered energy harvesting solutions are preferred.

At Secure Embedded Systems lab, **Deepak Mane**, **Krishna Pabbuleti** and **Patrick Schaumont** designed and prototyped an autonomous, self-powered wireless sensor node which can harvest energy from ambient sources. The sensor node consists of an MSP430, a low-power 8-bit microcontroller from TI which runs the signature algorithms and a 2.4GHz RF transceiver for communicating with the central server. The system harvests its energy from a solar panel and stores it in a super-capacitor. Energy harvesting and system power supply are managed by a custom-built IC from Anagear. Energy measurement infrastructure is also integrated in the system which can be used to measure the amount of energy consumed for computation and communication for different algorithms.

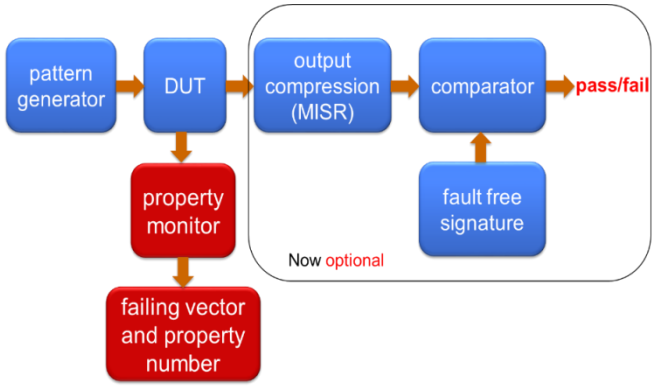
Energy consumption trends for three different signature schemes namely, ECDSA, Lamport-Diffie one-time hash-based signature scheme (LD-OTS) and Winternitz one-time hash-based signature scheme (W-OTS) are analyzed on this system. Though a trade-off was observed between computation energy and communication energy depending on the choice of algorithm and security level, the total energy consumption of different signature algorithms are within one order of magnitude.

The CESCA website includes a video that demonstrates the energy-harvesting signature system in operation (http://www.cesca.centers.vt.edu/Research/videos/index.html#v003).



Experimental setup showing solar panel (upper left), Anagear harvesting board (top), MSP430 DSP board (middle) and energy measurement unit (middle-left)

Diagnosis-Friendly LBIST Architecture Offers High Diagnostic Resolution



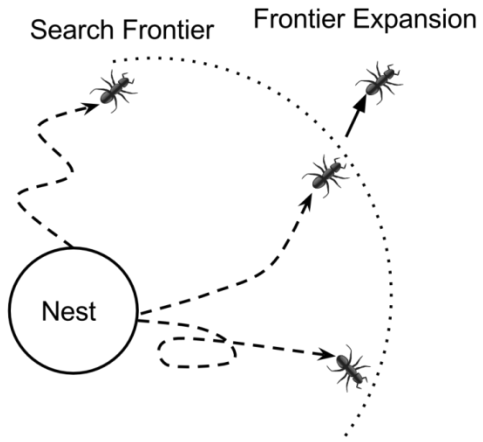
Logic built-in-self-test (BIST) is an on-chip test methodology that enables a chip to test itself. LBIST offers a number of benefits, including the elimination of automatic test equipment (ATE) and at-speed testing of circuits. However, the compressed responses make diagnosis extremely difficult. A diagnosis-friendly LBIST architecture can render LBIST to be more widely adoptable. CESCA faculty member **Michael Hsiao** and CESCA student **Sarvesh Prabhu** propose the use of hardware property monitors to improve the diagnosability in LBIST.

In this proposed architecture invariants in the fault free responses are extracted and used as property monitors. During the test session if any property is violated then the failing vector and property number is stored for offline diagnosis. Experimental results have shown that the architecture is able to achieve diagnosis resolution similar to that in a non-BIST setup.

Hybrid Deterministic-Stochastic RTL-level Validation achieves nearly 5X performance boost

Design Validation is a significant investment in today's design process. Register Transfer Level (RTL) validation focuses on ensuring behavior correctness of design descriptions before gate-level compilation and post-silicon debugging. A common metric for evaluating generated tests at the RTL is branch or line coverage, since at 100% coverage a test exists for every branching condition in the program. Random test generation often fail to provide adequate coverage of

the circuit under test in the presence of hard to reach corner cases and other highly specific behavior.



CESCA Faculty **Michael Hsiao** and CESCA student **Kelson Gent** built a hybrid deterministic + stochastic system for the automatic generation of RTL test patterns targeting branch coverage. The stochastic algorithm is primarily built on the ant colony optimization, a swarm intelligence algorithm that mimics the food gathering behavior of an ant colony. The algorithm is hybridized with a Satisfiability Modulo Theorem (SMT) based Bounded Model Checker (BMC) to aid in the navigation of potentially narrow paths by performing **frontier expansion** based on the current best known states of the ant colony. Additionally, the BMC was used to identify unreachable branches within the circuit. This method provided improved coverage and performance of nearly 5X over previous techniques.

VT ECE Embedded Systems at the Cornell Cup sponsored by Intel

A team of 5 ECE students (3 of them CESCA members) are a finalist team in the Cornell Cup sponsored by Intel (http://www.systemseng.cornell.edu/intel/). This national competition hosts 30 teams from different Universities in a showcase of the best Embedded Systems Engineering talent. The entry of Envision – the team of VT – in this competition is called the Interactive Vision Assistant. It is an interactive, portable system to assist the blind in outdoor navigation, by offering intelligent feedback about the surroundings in addition to providing directional guidance. But, the system is not restricted to plain old navigation and obstacle detection. It tries to make the user as much aware of his surroundings as possible by offering information – like "Hey! There goes your friend Jack." or "You probably should grab a coat today!" This means IVA must have real-time, advanced image processing and face recognition, as well as speech-conversion and internet connectivity. The IVA prototype is implemented on an Intel DE2i-150 board, an Intel Galileo board, several ultra-sonic sensors, a webcam, an accelerometer, GPS, and more. It can offer navigation, obstacle detection, people/face detection, and fall detection. Envision's blog (http://blogs.cornell.edu/cornellcup2014envision/) illustrates some of the current capabilities of IVA. We're rooting for their success at the final competition in Orlando, Florida on May 1st!

New Project

Dr. Lynn Abbott received an award from NASA Goddard Space Flight Center in the area of remote sensing. The goal of the project is to investigate the "Automated Detection of Ground and Top-of-Canopy Layers using Photon-counting Laser Altimetry." Abbott works closely with on this project with CESCA Ph.D. student Mahmoud Awadallah. The goal is to develop new techniques for analyzing lidar data that will be captured by a sensor known as ATLAS, from the ICESat-2 satellite. ICESat-2 is scheduled for launch in 2017.

Faculty Highlights

Park awarded COE Faculty Fellow

Dr. Jerry Park was selected as one of the recipients of the 2014 **College of Engineering Faculty Fellow** award. This award acknowledges and rewards tenure-track faculty in junior ranks who have shown exceptional merit in research, teaching and/or service. These awards are primarily aimed at associate professors.

Wang to teach in 2014 SAT/SMT Summer School

Dr. Chao Wang has been invited to give lectures in the 2014 SAT/SMT Summer School in Semmering, Austria, July 10-12 (http://satsmt2014.forsyte.at/). The Summer School aims at providing graduate students and researchers from universities and industry with a comprehensive overview of research and methodology in satisfiability testing (SAT) and satisfiability modulo theories (SMT). The lectures cover the foundational and practical aspects of SAT and SMT technologies and their applications. This will be the fourth in a series that includes the summer schools that took place at MIT in 2011, at Fondazione Bruno Kessler in Trento, Italy in 2012, and at Aalto University in Espoo, Finland in 2013. Dr. Wang's lectures will be focused on some of the exciting new applications of SAT/SMT solvers that he is currently working on, for example, automated verification and synthesis of concurrent software and cryptographic software.

Invited talk at Xilinx Emerging Technology Symposium by Schaumont

Xilinx, the market leader in Field Programmable Hardware Solutions, organizes a bi-annual research event for its top research workforce to discuss the recent progress in research domains important to Field Programmable Gate Arrays. **Dr. Patrick Schaumont** presented an invited talk on "Long Term Security for Fast Paced Technology," which addressed the paradox of building systems that have long-term trustworthiness in a world where technology generations are measured in months.

Invited presentations on Fingerprint Analysis by Abbott

Dr. Lynn Abbott attended the annual IAI International Educational Conference, which was held in Providence, Rhode Island, in August 2013. The IAI (International Association for Identification) is a professional association for those engaged in forensic identification, investigation, and scientific examination of physical evidence. Abbott gave an invited talk on "Feature Extraction and Temporal Analysis for Partial Fingerprint Identification," describing results of a recent NIJ-funded collaboration with **Dr. Michael Hsiao** of CESCA, Ed Fox of Computer Science, and recent Ph.D. CESCA graduate **Nathan Short**. Abbott was later invited by RTI International to deliver similar presentations as webcasts to IAI members. Two webcasts were held, in September and October, with average audiences of at about 90 individuals.

Schaumont guest-edits Special Issue on Embedded Platforms for Cryptography in the Coming Decade.

With collegues Tim Gueneysu (Ruhr University Bochum) and Maire O'Neill (Queen's University Belfast), **Dr. Patrick Schaumont** will assemble a special issue for ACM Transactions on

Embedded Computing Systems. Cryptography has made great strides in capability and variety over the past few years, enabling a broad range of new applications and extending the reach of security deep into the embedded world. This special issue of ACM Transactions on Embedded Computing Systems solicits state-of-the-art research results and surveys in embedded system engineering for novel cryptographic primitives for privacy and pervasive security, including for example lightweight primitives, lattice-based crypto-engines, cryptographic sponges, and homomorphic primitives. The submission deadline is July 1st, 2014 and the call for papers can be consulted at http://acmtecs.acm.org/.

Hsiao serves Technical Program Chair at HOST 2014

The IEEE Hardware Oriented Security and Trust Symposium (HOST) has become a premier forum for researchers to present and exchange novel ideas for hardware security and trust. **Dr. Michael Hsiao** is serving as the Program Chair (with Miodrag Potkonjak as Program Co-Chair and Farinaz Koushanfar as General Chair) for the symposium, which will take place May 6-7, 2014, in Arlington, VA. More information can be found at www.**host**symposium.org.

CESCA Seminars

CESCA Seminars in Spring 2014

CESCA seminars are held on weekly basis during the semester, and are held in Lavery Hall 320 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 speakers are open to everybody. Please join us!

- 2/7/14: Dr. Dongyoon Lee, Department of Computer Science at Virginia Tech, “Holistic System Design for Deterministic Replay”
- 2/21/14: Sarvesh Prabhu, Ph.D. Candidate, Department of Electrical & Computer Engineering at Virginia Tech, “Property-Checking based LBIST for Improved Diagnosability”
- 3/7/14: **CESCA Coffee + Cake**
- 3/21/14: Dr. Mantu K. Hudait, Department of Electrical & Computer Engineering at Virginia Tech, “Extremely High Mobility CMOS Logic”
- 4/4/14: Dr. Chung-Hsing Hsu, Oak Ridge National Laboratory, “TUE (Total-power Usage Effectiveness), a New Energy-Efficiency Metric Applied at ORNL's Jaguar”
- 4/11/14: Dr. Dhruv Batra, Department of Electrical & Computer Engineering at Virginia Tech, “Hedging Against Uncertainty via Multiple Diverse Predictions”
- ***Upcoming 4/25/14***: Dr. Dushan Boroyevich, Dr. Rolando Burgos, and students from Center for Power Electronics Systems (CPES) at Virginia Tech.

- ***Upcoming 5/2/14***: Dr. Zijiang "James" Yang, Department of Computer Science at Western Michigan University, "Automated Fault Explanation for Software Regression Testing"
- ***Upcoming 5/8/14*** (Thursday, 2:30pm~ at Lavery Hall 350): Sylvain Guilley, TELECOM ParisTech, Paris, France, "Mathematical and Formal Methods for Secure Design and Evaluation against Physical Attacks"

Student News & Highlights

New Students

- Shengjian Guo, PhD student
- Naling Zhang, PhD student
- Bilgiday Yuce, PhD student
- Ege Gulcan, MS student
- Sherin Ghannam, PhD student
- Abhijit Sarkar, PhD student

Recent Graduation

- Behnam Bahrak (PhD, advisor: Park), Currently seeking a faculty position in Iran

Recent Publications

- A. Aysu, E. Gulcan, P. Schaumont, "SIMON Says: Beat Area Records on FPGA," *IEEE Embedded Systems Letters*, to appear.
- A. Aysu, P. Schaumont, "PASC: Physically Authenticated Stable-Clocked SoC Platform on Low-Cost FPGAs", *2013 International Conference on Reconfigurable Computing and FPGAs*, December 2013.
- A. E. Youssef, A. S. Ibrahim, and A. L. Abbott, "Automated Gender Identification for Arabic and English Handwriting," *Proceedings: Fifth International Conference on Imaging for Crime Detection and Prevention* (ICDP-13), London, UK, Dec. 2013. (Received Best Poster award.)
- A. Maiti, P. Schaumont, "The Impact of Aging on a Physical Unclonable Function", *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, PP(99), 1.
- B. Bahrak and J. Park, "Coexistence decision making for spectrum sharing among heterogeneous wireless systems," *IEEE Transactions on Wireless Communications*, 13(3), 1298-1307.
- Chao Wang and Kevin Hoang, "Precisely deciding control state reachability in concurrent traces with limited observability," *International Conference on Verification, Model Checking, and Abstract Interpretation (VMCAI'14).* San Diego, CA. 2014.

- Hassan Eldib, Chao Wang, Mostafa Taha, and Patrick Schaumont. "QMS: Evaluating the side-channel resistance of masked software from source code," *ACM/IEEE Design Automation Conference (DAC'14).* San Francisco, CA. 2014.
- Hassan Eldib, Chao Wang, and Patrick Schaumont. "SMT-based verification of software countermeasures against side-channel attacks," *International Conference on Tools and Algorithms for Construction and Analysis of Systems (TACAS'14).* Grenoble, France. 2014.
- J. Park, J. Reed, A. A. L. Beex, T. C. Clancy, V. Kumar, and B. Bahrak, "Security and enforcement in spectrum sharing (invited paper)," *Proceedings of the IEEE*, 102(3), 270-281.
- K. Bian, J. Park, L. Chen, and X. Li, "Addressing the hidden terminal problem for heterogeneous coexistence between TDM and CSMA networks in white space," *IEEE Transactions on Vehicular Technology*, PP(99), 1.
- K. Bian, J. Park, X. Du, and X. Li, "Enabling fair spectrum sharing: Mitigating selfish misbehaviors in spectrum contention," *IEEE Network*, May/June 2013, pp. 16–21.
- Kelson Gent and Michael S. Hsiao, "Functional test generation at the RTL using swarm intelligence and bounded model checking," *Proceedings of the IEEE Asian Test Symposium*, November 2013.
- Kuan-Yu Liao, Ang-Feng Lin, James C.-M. Li, Michael S. Hsiao, and Laung-Terng Wang, "GPU-based timing-aware test generation for small delay defects," *Proceedings of the IEEE European Test Symposium*, May 2014.
- M. Awadallah, A. L. Abbott, V. Thomas, R. H. Wynne, and R. Nelson, "Estimating Forest Canopy Height and Biophysical Parameters using Photon-counting Laser Altimetry," *Proceedings: 13th International Conference on LiDAR Applications for Assessing Forest Ecosystems* (SilviLaser 2013), Beijing, China, Oct. 2013.
- M. Awadallah, S. Ghannam, A. L. Abbott, and A. Ghanem, "Active Contour Models for Extracting Ground and Forest Canopy Curves from Discrete Laser Altimeter Data," *Proceedings: 13th International Conference on LiDAR Applications for Assessing Forest Ecosystems* (SilviLaser 2013), Beijing, China, Oct. 2013.
- M. Taha and P. Schaumont, "Side-Channel Countermeasure for SHA-3 at Almost-Zero Area Overhead", *IEEE Symposium on Hardware Oriented Security and Trust* (HOST 2014), Arlington, VA, May 2014.
- Mahmoud Elbayoumi, Michael S. Hsiao and Mustafa Elnainay, "Selecting critical implications with set-covering formulation for SAT-based bounded model checking," *Proceedings of the IEEE International Conference on Computer Design*, October 2013.
- Mahmoud Elbayoumi, Mihir Choudury, Victor Kravets, Michael S. Hsiao, and Mustafa Elinainay, "TACUE: A Timing-Aware Cuts Enumeration Algorithm for Parallel Synthesis," *Proceedings of the IEEE Design Automation Conference, June 2014*.

- N.F. Ghalaty, A. Aysu, P. Schaumont, "Analyzing and Eliminating the Causes of Fault Sensitivity Analysis", *Design, Automation & Test in Europe* (DATE 2014), Dresden, Germany, March 2014.
- R. Kannavara, P. Schaumont, M. Maniatakos, M. A. Smith, S. Buck, "Innovative Engineering Outreach Using Intel Security and Embedded Tools," *10th European Workshop on Microelectronics Education*, May 2014.
- S. Ghannam and A. L. Abbott, "Cross Correlation versus Mutual Information for Image Mosaicing," *International Journal of Advanced Computer Science and Applications* (IJACSA), 4(11).
- Sarvesh Prabhu, Vineeth V. Acharya, Sharad Bagri and Michael S. Hsiao, "Property-checking based LBIST for improved diagnosability," *Proceedings of the IEEE European Test Symposium*, May 2014.