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

March 2012• No.007

In this edition:

NSF CAREER Awards for Chao Wang and Yaling Yang

Two CESCA members, Dr. Chao Wang and Dr. Yaling Yang, have received Faculty Early Career Development (CAREER) awards from the National Science Foundation. These prestigious awards are given to creative junior faculty who are likely to become academic leaders of the future.

Dr. Chao Wang

Dr. Wang, who is in his first year as a faculty member at Virginia Tech, will use his five-year, $478,000 award to address the complex problem of debugging computer software. Detecting and fixing software defects, or bugs, has become extremely labor-intensive because of the rapidly increasing size and complexity of today's software.

Dr. Yaling Yang

The rapid acceptance of multicore processors has exacerbated the problem of code development and debugging. Concurrency-related bugs are particularly difficult to diagnose and fix. According to Wang, "Automation of this bug detection and repair process promises to drastically reduce the time spent on debugging such systems, leading to more reliable and secure software as well as fully utilized parallel hardware." Wang's research will seek to dramatically improve the reliability and security of software systems through innovations in automated concurrency debugging.

Dr. Yang's five-year award, for $450,000, will support her work on cross-layer incompatibility issues that disrupt delivery on wireless networks. She will analyze the networks to identify incompatibilities that slow network delivery and design practices for compatibility. The grant will help her to categorize and analyze over-burdened wireless networks.

Yang likens the design of networks to the popular Tetris computer game, with the networking functions serving as the moving building blocks that should fit together like a puzzle. When the building blocks fit together correctly, data packets are able to travel smoothly through the network. In recent years, however, because of the drive to boost wireless network performance, many network designs have deviated from the traditional one-layer building blocks to more complex multi-layer designs. Thus, ensuring that all these pieces fit together has become a challenge.

"The objective of this project is to systematically and rigorously categorize and analyze coexistence restrictions of cross-layer designs in wireless networks," Yang writes in her abstract of the study. "In this project, coexistence restrictions of various cross-layer designs are theoretically modeled and analyzed. Different kinds of coexistence restrictions are defined, the conditions for their occurrences and their impact on network operations are revealed, and methods to check coexistence issues are developed." The study also seeks to create restriction-compliant protocol designs, or making sure all cross-layers are uniform and the packets of data can pass unencumbered through the networks. "Ultimately, this will greatly enhance the flexibility and robustness of current and future wireless network systems."

From the Director's Desk

Another year has passed since we published our last newsletter. We have all been busy with developing our research portfolio, courses, summer industrial courses, and student graduations, and possibly ignored one important part of running a center – publicity. So eventually, thanks to Lynn Abbott, we are publishing our accomplishments of 2011 in a single newsletter – rather than in installments of three newsletters for summer, fall and spring. We plan to be more regular in 2012, with hopefully with at least two newsletters per year.

There are several news items that we are particularly proud of. First, our research expenditure for 2011 financial year was more than two million dollars which is a goal we strived to achieve since our very inception. In the last 5 years, our research expenditure has always followed an upward trend, going from $1.4 M to $1.7 M in 2009 and 2010, respectively, and now it has reached a coveted benchmark. Research expenditure of a center is a metric that reflects a measure of research activity at the center, because it comprises the wages of GRAs, undergraduate research assistants, and salaries of postdoctoral researchers, as well as expenditures on equipment and travel. In that measure, we are showing signs of good health, and we hope to see more growth in this metric. Second, two of our junior faculty were awarded the much coveted NSF CAREER award. This brings the total of seven CAREER awards in CESCA which I believe is unparalleled for any center in Virginia Tech, and possibly even outside Virginia Tech. We are very proud that we have created an environment of mutual cooperation and nurturing among the various faculty and their respective research groups, and this has fostered a healthy competitiveness in striving for such honors.

On the publication front for the academic year ending in 2011, we have published 1 book, 5 book chapters, 44 peer-reviewed conference papers, and 16 journal papers. We graduated 15 students, 6 of whom were PhDs. In summary, 2011 has continued the trend of the past so many years of CESCA. We also added a new faculty member – Dr. Chao Wang, who joined CESCA in fall 2011 after 7 years of experience in an industrial research lab. We believe that his industrial and academic experience will contribute heavily in CESCA's continued striving for excellence in research and education, as well as in it funding portfolio, graduation of students, and publications.

In 2011, we celebrated CESCA students and faculty on CESCA day by organizing an all day workshop where all CESCA students displayed glimpses of their work in poster sessions, and we got to hear various speakers talk about research, personal development, and time management. This year, the CESCA day event will be held on April 21st, and we are looking forward to see the excited faces of our students explaining their most recent research accomplishments during the poster sessions. We are also lucky to have Prof. Douglas Schmidt visit from Vanderbilt University to deliver the keynote speech at this event.

Another important piece of news is that CESCA has inaugurated a completely new website. The new site is based on a content management system run by the University, and which is a product of the tireless supervision of Prof. Dong Ha, with the help of his administrative assistant Ms. Yumi Lim.

Before I close my column, I must thank all CESCA faculty, postdoctoral researchers, and students for making CESCA a great place to work, and a great environment for academic nurturing. Last but not the least, I must thank Ms. Yumi Lim for her excellent work for CESCA – on making sure all the administrative machinery is running well and healthy, and for creating all the CESCA displays around the third floor of Durham Hall.

Dr. Sandeep Shukla, director

Welcome to New Member

Dr. Chao Wang

CESCA is delighted to introduce Dr. Chao Wang as its newest faculty member. Dr. Wang joined the Bradley Department of Electrical and Computer Engineering in August, 2011, after working for several years in industry.

Wang earned bachelor's and master's degrees in Electrical Engineering from Peking University in China in 1996 and 1999, respectively, and then a doctoral degree (also in Electrical Engineering) from the University of Colorado at Boulder in 2004. From 2004 to 2011, he worked as a research staff member at NEC Laboratories Inc. in Princeton, N.J.

Dr. Wang's research interests include automated verification, software engineering, and programming languages. As noted on page 1 of this newsletter, he recently received an NSF CAREER award to support research in concurrent software debugging.

Courses for Industry taught by CESCA Faculty

Part of the excitement, as well as the challenge, of an engineering career is to stay up to date with the latest developments in the field. Last summer, CESCA helped professional computer engineers to learn about secure and trustworthy hardware and software. Three CESCA Faculty organized two courses in collaboration with Virginia Tech's Center for Continuing Education. The courses were organized two times, the first time in Virginia Tech's Northern Virginia campus, and the second time on-location for a company sponsor.

The first course was a three-day course on Hardware Security, taught by Dr. Patrick Schaumont. This course described the key concepts in secure hardware design, including technologies for secure hardware, design techniques for cryptographic implementations, and design techniques for trustworthiness. The second course was a three-day course on Software Assurance, taught by Dr. Sandeep Shukla and Dr. Michael Hsiao. This course introduced formal and informal methods for test generation, abstraction techniques to build formal models, secure programming, major threat models or security lapses in software, and techniques to locate security bugs.

Due to the success of this program, CESCA faculty is currently developing a curriculum for the summer of 2012. Besides the courses on hardware security and software assurance, two new courses will be offered. One course will be on Principles and Practice of Energy Harvesting, and it will be taught by Dr. Ha. This course reviews principles of energy harvesting and practices for small scale energy harvesters developed recently. The second course will be on Hardware/Software Codesign with platform FPGA. This course will be taught by Dr. Schaumont, and covers hardware/software integration techniques for the latest generation of FPGA's.

The courses include presentations as well as hands-on assignments. This way, participants have a chance to experience theory and practice in a single course. At the end of the course, the participants receive a certificate, allowing them to use the course to fulfill part of the training requirements in a Professional Engineering Degree.

Full details can be found at the course website at http://rijndael.ece.vt.edu/cescacourse/.

CESCA Demonstrates First SHA-3 Silicon

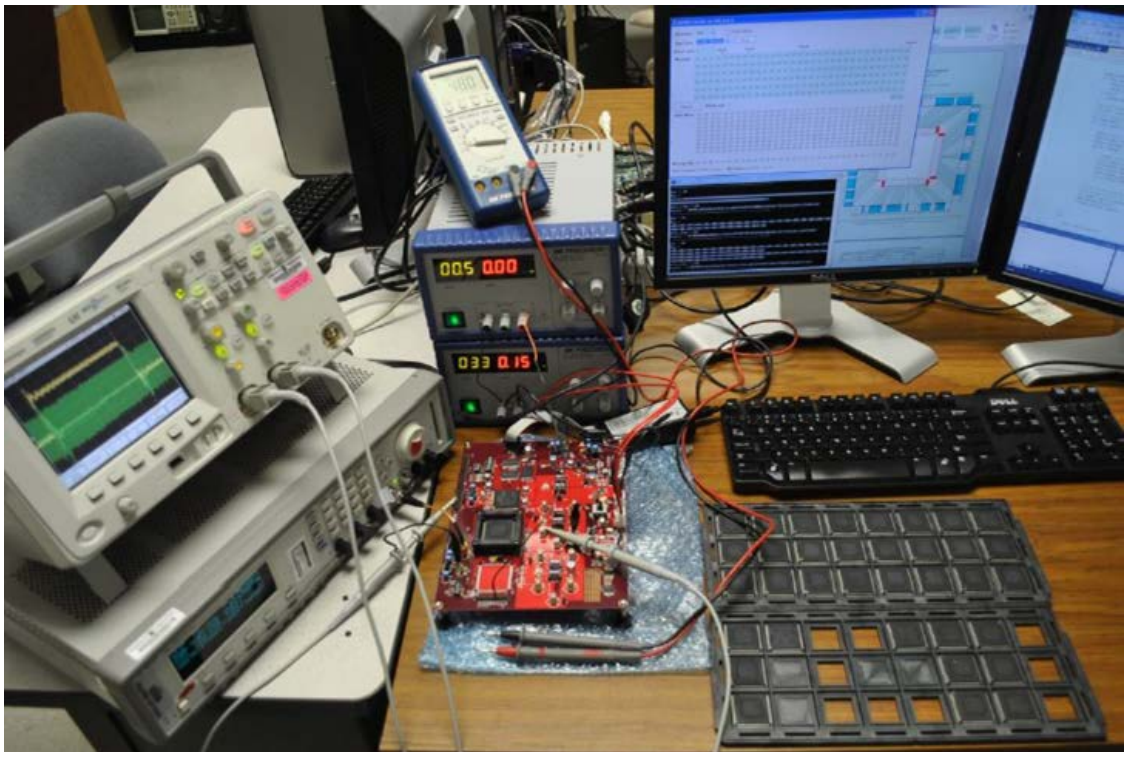
CESCA is participating in the creation of a new cryptographic hashing standard, and they demonstrated the first working silicon for this standard.

Modern cryptographic standards are produced using a competition process. One ongoing competition is being organized by NIST, the National Institute of Standards and Technology, and it involves a new cryptographic hash standard, called SHA-3. Hashes are used as part of many modern cryptographic protocols. For example, they aid in the generation of signatures, in the creation of integrity checksums, and in the authentication of messages. In order to select the right hash algorithm as the next SHA-3 standard, NIST evaluates many aspects among competing proposals, including for example perceived cryptographic strength, performance in software, and efficiency in hardware.

A CESCA team, under guidance of Dr. Schaumont and Dr. Nazhandali, is taking charge of the evaluation of the ASIC hardware efficiency of the final five hash proposals. The design of an ASIC chip is the final step in the evaluation process. The ASIC, which was implemented in 130nm CMOS standard cells, includes 6 different algorithms, and has been optimized to test the algorithms under various operating conditions. The ASIC was manufactured in February 2011, and it was extensively tested over the summer of 2011.

In the fall of 2011, the chip was distributed to 9 international research labs, including Bristol University (UK), NIST (USA), Ruhr University Bochum (GE), University of Electro-Communications (JP), TU Darmstadt (GE), City University of Hong Kong (Hong Kong), AIST (JP), COSIC (BE) and TU Munich (GE). The chip is the first chip that implements the SHA-3 finalist candidates. Since NIST is planning to decide on the winning hash algorithm in the second quarter of 2012, it is important to gather design evaluation data as early as possible. The chip design is fully documented at the SHA3-VT website (http://rijndael.ece.vt.edu/sha3).

The CESCA students involved in this project include Xu Guo, Meeta Srivastav, Yongbo Zuo, Sinan Huang, Francisco Borelli, Dinesh Ganta, and Michael Henry.



MEMOCODE coming to Virginia Tech

Virginia Tech Research Center at Arlington, Virginia, will host the 10th ACM/IEEE International Conference on Formal Methods and Models for Co-Design (MEMOCODE 2012). It is technically sponsored by ACM and IEEE, and is financially sponsored by several organizations, including the Bradley Department of Electrical and Computer Engineering of Virginia Tech.

In the past, MEMOCODE conferences featured many visionary researchers in the field as keynote speakers – they include Tony Hoare, Edmund Clarke, Amir Pneuli (all Turing Awardees), Edward Lee, Alberto Sangiovanni Vincentelli, Kenneth McMillan, David Dill, Nicholas Halbwach, Daniel Gajski, Satnam Singh, among others.

This conference has gained quite a visibility since its inception in 2003 (started by Sandeep Shukla, Jean-Pierre Talpin and Rajesh Gupta) because of its unique nature in combining design with methodology -- especially formal methodology in design. Past occurrences of MEMOCODE were hosted at Microsoft Research, Verimag, INRIA Rennes, INRIA Sophia-antipolis, MIT, University of Verona, UC San Diego. Many of the CESCA faculty and students have expertise in the core areas of this conference, and we hope that CESCA will participate at the conference in large numbers.

For more information, you could check out this year's conference website: http://memocode.irisa.fr/2012/MEMOCODE%202012.html.

CESCA Seminar Series and Video Channel

CESCA continues to hold regular research seminars, and to make most of them available on the CESCA video channel *http://vimeo.com/channels/cesca*. The topics in Fall 2011 and (so far) in Spring 2012 were as follows:

- Christian Colombo (University of Malta), "*Handling Runtime Monitoring Overhead*"
- Sandeep Shukla (VT), "*Software Systems as Complex Networks*"
- Yaman Evrenosoglu (VT), "*An Insight to Contemporary Power Systems*"
- Jean-Pierre Talpin (INRIA), "*Polychrony as an Abstract Model of Computation*"
- Malay Ganai (NEC Labs), "*Predicting Run-time Errors in x86 Executables of Multi-threaded C/C++/Java Programs*"
- ZhiChun Li (NEC Labs), "*Towards Scalable User-Agnostic Attack Defense*"
- Georg Weissenbacher (Princeton University), "*SAT-based Design Debugging and Fault Localization*"
- Rajeev Alur (University of Pennsylvania), "*Interfaces for Control Components*"
- Kenneth Schulz (Lockheed Martin), "*Overview of RC ICs: Industry Perspective*" (CESCA/IEEE joint seminar)
- Michael Hsiao (VT), "*Sufficiency-based Framework for Sequential Equivalence Checking*"
- Patrick Schaumont (VT), "*Moving PUFs out of the Lab*"
- Lynn Abbott (VT), "*How to Analyze Low-Quality Fingerprint Images*"
- Bo Gao (VT), "*Uplink Soft Frequency Reuse for Self-Coexistence of Cognitive Radio Networks Operating in White-Space Spectrum*"
- Gyungsu Byun (West Virginia University), "*Energy-efficient Dual-band Interconnect for Future Mobile Computing Systems*"

CESCA gratefully acknowledges the students of its Multimedia Task Force, who produce video recordings of all major CESCA events. These include Shaver Deyerle, Mahesh Nanjundappa, Nathan Short, Abhranil Maiti, Yi Deng and Ambuj Sinha.

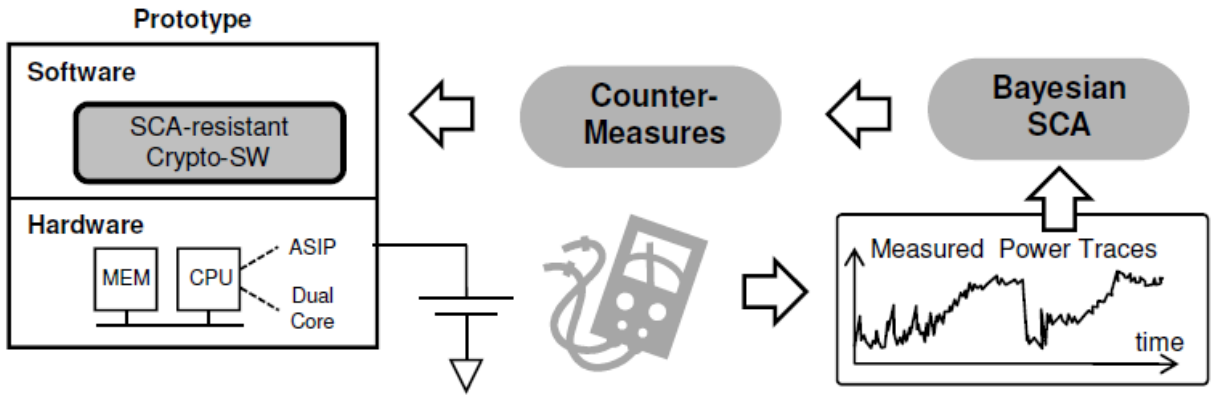
New Research Projects

New Directions in Side-channel Attacks and Countermeasures
In a cross-department collaboration, Inyoung Kim from the Statistics Department and Patrick Schaumont from CESCA received a $429K grant from the National Science Foundation to work on innovative side-channel attacks and countermeasures.

In a side-channel attack, an attacker captures the implementation effects of cryptography, such as power consumption and execution time. A distinctive feature of a side-channel analysis (SCA) attack is that it can reveal a small part of the secret-key. Hence, side-channel attacks avoid the brute-force complexity of cryptanalysis. Using novel side-channel estimation techniques based on Bayesian statistics, the project develops more powerful side-channel attacks.

The project also develops novel software-oriented countermeasures that more flexible and general than traditional hardware-oriented side-channel countermeasures. The efficiency of side-channel attacks and side-channel countermeasures are evaluated using hardware and software prototyping. The project combines advanced statistical techniques with advanced computer engineering, building synergy between Statistics and Computer Engineering.

The project will run for three years, and it will involve students from the Statistics Department as well as from the Bradley Department of Electrical and Computer Engineering.



- **Techniques for Physical-layer Signal Authentication**

Jerry (Jung-Min) Park received funding from L-3 Communications to investigate physical-layer signal authentication schemes. The critical role of spectrum as a catalyst for economic growth was brought forth in the recently announced National Broadband Plan. To achieve the ambitious goals of this initiative, a transition from the legacy "command-and-control" regulatory model (where spectrum is parceled and allocated to specific companies and applications) to a more flexible model of shared dynamic spectrum access is necessary. One of the critical challenges that needs to be addressed to realize the shared access model is the development of technologies for spectrum security and enforcement. This project will study physical (PHY)-layer authentication schemes that play an integral part in spectrum security and enforcement. While cryptographic mechanisms at the higher layers have been widely used to authenticate wireless transmitters, the ability to authenticate and uniquely identify transmitters at the PHY layer has key advantages over higher-layer approaches, particularly in heterogeneous coexistence environments where incompatible systems may not be able to decode each others' higher-layer signaling.

- **State Estimation Security in WAMS**

Sandeep Shukla announced a new project that is related to the prevention of cyber attacks. With the increasing incorporation of phasor-measurement units (PMUs), smart digital relays, and smarter control based on wide-area visibility, the modern transmission system is exposed to the cyber attack vulnerabilities that might lead to large-scale blackout. Our work focuses on finding cyber based attack scenarios on the WAMS based state estimation, finding ways to thwart such cyber attacks, quantifying the average loss if successfully attacked and altered estimated states and finding more robust state estimation techniques that would be harder to attack in these ways. The project is sponsored by the Hume Center's IUCRC affiliate General Electric.

- **Ha 's Team Awarded $1.2 Million from NSF on Building a New Sensor System for Fall Prevention**

Dong Ha teamed up with two other VT professors, Thurmon Lockhart (PI) and Karen Roberto, and with a professor from University of Virginia, and received a grant ($1.2M for four years) from NSF's Smart Health and Wellbeing Program. Their research investigates to develop a portable fall prediction monitoring system for early detection of fall risks that can provide early diagnosis / treatment before a fall occurs to reduce long-term health effects and injuries. Users would wear the device as a faux piece of jewelry on a piece of clothing or around an ankle. It will measure potentially small declining increments in gait, posture and mobility of a patient, major indictors that can help point to a future fall. Ha's team develops a wearable wireless sensor node, which senses the motion of a person and transmits the data to a host computer wirelessly. The major design object is to reduce the power dissipation of the sensor node without compromising the quality of key data captured.

Faculty Highlights

Michael Hsiao began a 2-year term (starting 2011) serving as an Associate Editor for the *IEEE Transactions on Computers.*

Patrick Schaumont is Program Co-chair for the 2012 Workshop on Cryptographic Hardware and Embedded Systems (CHES). The event is a premier forum for the latest developments in cryptographic hardware and embedded systems. CHES attracts over 350 attendees from academia, government and industry, and typically receives around 120 submissions. CHES 2012 will be organized in Leuven, Belgium.

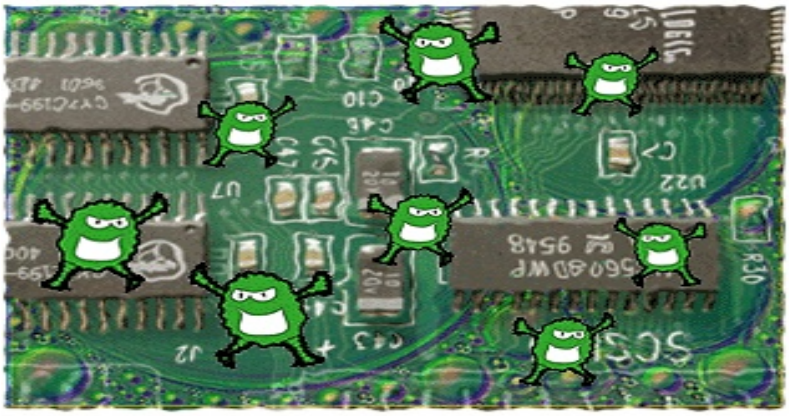
Patrick Schaumont begins a three-year term as associate editor for the *ACM Transactions on Design Automation of Electronic Systems*. He will cover the area of Dependable and Secure Computing.

Sandeep Shukla is the General Chair of the ACM/IEEE International Conference on Formal Methods and Models for Co-Design (MEMOCODE) to be held in Arlington, VA, July 16-18, 2012.

Sandeep Shukla is the Co-general Chair of the IEEE/ECSI International Symposium on Electronic System Level Synthesis (ESLsyn) to be held in San Francisco, CA, June 2-3, 2012.

Sandeep Shukla is now an Associate Editor of the *Journal of Computing,* published by the Computer Society of India. He also started another 2 year term as Associate Editor of *IEEE Transactions on Computers*, and just finished his 4 terms as an Associate Editor of *IEEE Design & Test*.

ICTAS Workshop on Trusted Hardware



A one-day workshop was held at the Inn at Virginia Tech in November 2011, with a focus on Trusted Hardware. Michael Hsiao (CESCA) and Jon Greene (ICTAS) co-organized the event. The intent of the forum was to seek innovative solutions to this challenge. While much effort has been devoted to network and software security in the past, the issue of trusted hardware is an area that currently needs more comprehensive solutions. The desired outcome is to nucleate powerful interdisciplinary teams and approaches to hardware trust, including tacking anti-tamper, anti-counterfeiting, and so on. A number of CESCA faculty and students participated in the event, and together brainstormed several key ideas on the problem, which are being researched.

Best Paper Awards

Best Paper Award for PUF Research at FPGA Conference

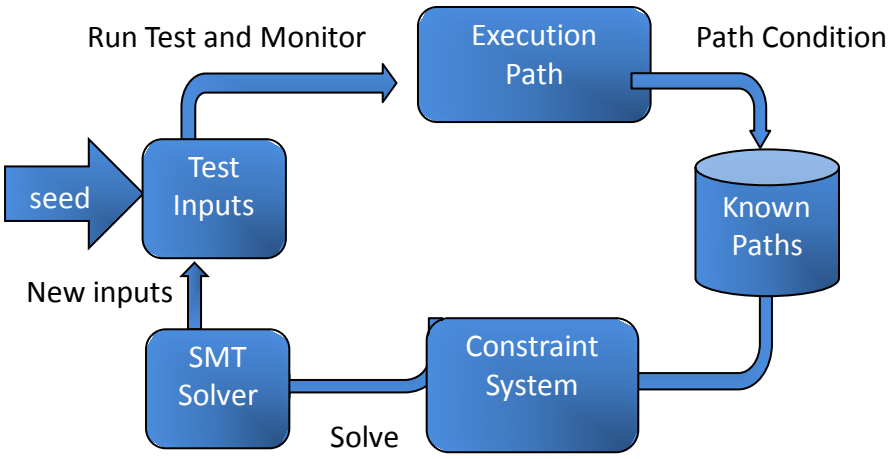
Abhranil Maiti, CESCA Ph.D. student, received a best paper award at the 21st International Conference on Field Programmable Logic and Applications (FPL). The presented paper as entitled "The Impact of Aging on an FPGA-based Physical Unclonable Function," and it was co-authored by Logan McDougall, CESCA undergraduate student, and Dr. Patrick Schaumont. FPL is the first and largest conference on field programmable logic. FPL 2011 received 213 submissions.

In this paper, the researchers investigated the effects of aging on a particular cryptographic circuit called a Physical Unclonable Functions (PUF). PUFs are used as a means to implement hardware identifiers. For example, they can be used to authenticated a single chip, or to generate a unique cryptographic key. Naturally, identity is something that one expects to remain constant over the lifetime of the chip. This makes the study of aging effects important. The conclusions of the paper are counter-intuitive. First, the researchers observed that, due to circuit aging, the electronic identity of a chip becomes noisy. Second, they observed that the electronic identity of the

chip remains distinguishable compared to the identity of other chips. The former conclusion means that more work is needed to make chip identifiers stable. The latter conclusion is good news: it means that PUFs are useful despite the existence of aging effects.

Best Paper Award at the Asian Test Symposium in 2011

The paper, "Tackling the path explosion problem in symbolic execution-driven test generation", was authored by Saparya Krishnamoorthy, Michael S. Hsiao, and Loganathan Lingappan. In this paper, novel search strategies for symbolic testing software were proposed. Traditional symbolic techniques have failed to scale to large programs due to the exponential number of paths to be explored. In this paper, the authors achieved complete branch coverage under symbolic execution, while exploring only a fraction of paths in the program. A clever use of the reachability graph of the program to explore unvisited portions of the program and a powerful conflict-driven backtracking strategy were developed to achieve these goals.



Student News

Who graduated?

Name	Degree	Where they will go
Kaigui Bian	Ph.D.	Peking University
Zhimin Chen	Ph.D.	Microsoft Research
Amol Deshpande	M.S.	ViaSat
Khanh Duong	M.S.	NVidia
Donald Hanle	M.S.	Amentra
Mike Henry	Ph.D.	Currently teaching at VT
Kevin Hoyle	M.S.	G3 Technologies
Wei Hu	M.S.	Bloomberg
Srikrishna Iyer	M.S.	Qualcomm
Bijoy Jose	Ph.D.	Intel
Swati Kanaujia	M.S.	Microsoft
Jeong Ki Kim	Ph.D.	Korea Communications Commission
Na Kong	Ph.D.	Texas Instruments
Chinmay Limaye	M.S.	Intel
Supratik Misra	M.S.	NVidia
Huy Nguyen	M.S.	Freescale
Sarvesh Prabhu	M.S.	Ph.D. student at VT
Ambuj Sinha	M.S.	Advanced Simulation Technology
Jatin Thakkar	M.S.	Deutsche Bank
Bin Xue	Ph.D.	NVidia
Jinsik Yun	M.S.	Qualcomm

Internships

- Dhrumeel Bakshi, Intel
- Min Li, Bloomberg
- Supratik Misra, Intel

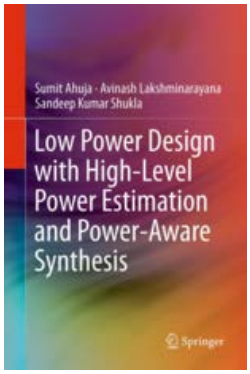
Publications

- K. Bian, J. Park, and R. Chen, "Control channel establishment in cognitive radio networks using channel hopping," *IEEE Journal on Selected Areas in Communications*, Vol. 29, No. 4, April, 2011, pp. 689-703.
- networks operating in white-space spectrum," IEEE Annual Int'l Conference on Computer Communications (INFOCOM), Mar. 2012.
- B. Gao, Y. Yang, and J. Park, "Channel aggregation in cognitive radio networks with practical considerations," IEEE International Conference on Communications (ICC 2011), Kyoto, Japan, June, 2011.
- K. Bian and J. Park, "Asynchronous channel hopping for establishing rendezvous in cognitive radio networks," 2011 IEEE INFOCOM Mini-Conference, Apr. 2011.
- Shravan Garlapati, and Sandeep Shukla, “Optimum Location of Master Agents in an Agent Based Zone 3 Protection Scheme Designed for Robustness Against Hidden Failure Induced Trips to the Submission Site”, accepted for presentation at the PES General Meeting, July 2012
- Soumyo Chakraborty, Sandeep Shukla and Jim Thorp, “System Imbalance Minimizing Renewable Generation Portfolio Selection in the Presence of Plug-in Electric Vehicles”, accepted for presentation at the PES General Meeting, July 2012
- Soumyo Chakraborty, Sandeep Shukla and Jim Thorp, “A Detailed Analysis of the Effective-Load-Carrying-Capacity Behavior of Plug-in Electric Vehicles in the Power Grid”, to appear in the proceedings of the 2012 IEEE PES Conference on Innovative Smart Grid Technologies, Washington DC, January 2012
- Jens Brandt, Mike Gemuend, Klaus Schneider, Sandeep Shukla, and Jean-Pierre Talpin, “Integrating System Descriptions by Clocked Guarded Actions”, To appear in the proceedings of International Forum on Design Languages (FDL’11), September 2011, Oldenburg, Germany.
- Yi Deng, Hua Lin, Sandeep Shukla, Jim Thorp, Lamine Mili, “Communication Network Modeling and Simulation for Wide Area Measurement Applications”, to appear in the proceedings of the 2012 IEEE PES Conference on Innovative Smart Grid Technologies, Washington DC, January 2012.
- Bijoy A. Jose, Abdoulaye Gamatie, Julien Ouy and Sandeep K. Shukla, SMT Based False Causal loop Detection during Code Synthesis from Polychronous Specifications, accepted to be published in the proceedings of ACM/IEEE International Conference on Methods and Models for Co-Design (MEMOCODE’11), Cambridge, UK, July 2011, pp. 109-108, IEEE Computer Society Press.
- Avinash Lakshminarayana, Sumit Ahuja, and Sandeep Shukla, "High Level Power Estimation Models for FPGAs," IEEE Computer Society Annual Symposium on VLSI (ISVLSI), pp.7-12, July 2011.
- Soumyo V. Chakraborty, Sandeep K. Shukla, James Thorp, “Optimizing Grid Contribution and Economic Returns from Solar Generators by Managing the Output Uncertainty Risk”, proceedings of the 2011 IEEE Power Tech, Trondheim, Norway, June 2011.
- Soumyo V. Chakraborty, Sandeep K. Shukla, James Thorp, “A Framework For Analyzing Load-Carrying-Capacity Of Plug-In Electric Vehicles And Impact On Solar Generators”, proceedings of the 2011 IASTED European Conference on Power and Energy Systems, Crete, Greece, June 2011.

- S. Prabhu, M. S. Hsiao, L. Lingappan and V. Gangaram, “A novel SMT-based technique for LFSR reseeding,” in Proceedings of the IEEE VLSI Design Conference, January 2012.
- W. Hu, H. Nguyen, and M. S. Hsiao, "Sufficiency-based filtering of invariants for sequential equivalence checking," in Proceedings of the IEEE High Level Design Validation and Test Workshop, November 2011.
- M. Li, K. Gent and M. S. Hsiao, "Utilizing GPGPUs for design validation with a modified ant colony optimization," in Proceedings of the IEEE High Level Design Validation and Test Workshop, November 2011.
- S. Prabhu, M. S. Hsiao, S. Krishnamoorthy, L. Lingappan, V. Gangaram and J. Grundy, "An efficient 2-phase strategy to achieve high branch coverage," in Proceedings of the IEEE Asian Test Symposium, November 2011.
- M. Li and M. S. Hsiao, "Three-dimensional parallel fault simulation with GPGPU," in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 30, no. 10, October 2011, pp. 1545-1555.
- N. Short, A. L. Abbott, M. S. Hsiao, and E. Fox, "A Bayesian approach to fingerprint minutia localization and quality assessment using adaptable templates," in Proceedings of the International Joint Conference on Biometrics, October 2011.
- L.-T. Wang, N. A. Touba, M. S. Hsiao, J.-L. Huang, J. C.-M. Li, S. Wu, X. Wen, M. Bhattaraie, F. Li, and Z. Jiang, "Architectures for testing 3D chips using time-division demultiplexing/multiplexing," in Proceedings of the IEEE International Workshop on Testing Three-Dimensional Stacked Integrated Circuits, September 2011.
- S. Krishnamoorthy, M. S. Hsiao, and L. Lingappan, "Strategies for scalable symbolic execution-driven test generation for programs," in Science China Information Sciences, vol. 54, no. 9, pp. 1797-1812, 2011.
- S. H. Park, J. Leidig, L. T. Li, E. Fox, N. J. Short, K. E. Hoyle, A. L. Abott and M. S. Hsiao, "Experiment and analysis services in a fingerprint digital library for collaborative research," to appear in Proceedings of the International Conference on Theory and Practice of Digital Libraries, September 2011.
- M. Banga and M. S. Hsiao, "ODETTE: A non-scan design-for-test methodology for trojan detection in ICs," in Proceedings of the IEEE Hardware-Oriented Security and Trust Symposium, June 2011.
- M. Li and M. S. Hsiao, "High-performance diagnostic fault simulation on GPUs," in Proceedings of the IEEE European Test Symposium, May 2011.
- S. Wu, L.-T. Wang, X. Wen, Z. Jiang, L. Tan, Y. Zhang, Y. Hu, W.-B. Jone, M. S. Hsiao, J. C.-M. Li, J.-L. Huang, and L. Yu, "Using launch-on-capture for testing scan designs containing synchronous and asynchronous clock domains," in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 30, no. 3, March, 2011, pp. 455-463.
- M. Banga, N. Rahagude, and M. S. Hsiao, "Design-for-test methodology for non-scan at-speed testing," in Proceedings of the IEEE Design Automation and Test in Europe Conference, March 2011.
- X. Guo, M. Srivistav, S. Huang, D. Ganta, M. B. Henry, L. Nazhandali, and P. Schaumont, "ASIC Implementations of Five SHA-3 Finalists," Design, Automation and Test in Europe (DATE2012), March 2012.
- A. Maiti, V. Gunreddy, P. Schaumont, "A Systematic Method to Evaluate and Compare the Performance of Physical Unclonable Functions", IACR ePrint 2011/657, November 2011.
- X. Guo, P. Schaumont, "The Technology Dependence of Lightweight Hash Implementation Cost", Ecrypt II 2011 Workshop on Lightweight Cryptography, November 2011.
- Z. Chen, A. Sinha, P. Schaumont "Using Virtual Secure Circuit to Protect Embedded Software from Side-Channel Attacks," IEEE Transactions on Computers, preprint, 2011.
- S. Mane, L. Judge, P. Schaumont, "An Integrated Prime-field ECDLP Hardware Accelerator with High-performance Modular Arithmetic Units," 2011 International Conference on Reconfigurable Computing and FPGAs (RECONFIG), December 2011.
- A. Maiti, I. Kim and P. Schaumont, "A Robust Physical Unclonable Function with Enhanced Challenge-Response Set," IEEE Transactions on Information Forensics and Security, November 2011.

- A. Maiti, L. McDougall and P. Schaumont, "The Impact of Aging on An FPGA-Based Physical Unclonable Function," 21st International Conference on Field Programmable Logic and Applications (FPL 2011), September 2011. (Best Paper Award.)
- X. Guo, Meeta Srivistav, S. Huang, D. Ganta, M. Henry, L. Nazhandali, and P. Schaumont, "Pre-silicon Characterization of NIST SHA-3 Final Round Candidates", 14th Euromicro Conference on Digital System Design Architectures, Methods and Tools (DSD 2011), August 2011.
- S. Iyer, J. Zhang, Y. Yang, and P. Schaumont, "A Unifying Interface Abstraction for Accelerated Computing in Sensor Nodes," 2011 Electronic System Level Synthesis Conference, San Diego, June 2011.
- J. Zhang, Y. Tang, S. Hirve, S. Iyer, P. Schaumont, Y. Yang, "A Software-Hardware Emulator for Sensor Networks," 8th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, June 2011. Best Paper Award.
- S. Morozov, C. Tergino, P. Schaumont, "System Integration of Elliptic Curve Cryptography on an OMAP Platform," 9th IEEE Symposium on Application Specific Processors, June 2011.
- X. Guo, M. Srivastav, S. Huang, D. Ganta, M. Henry, L. Nazhandali, P. Schaumont, "Silicon Implementation of SHA-3 Finalists: BLAKE, Groestl, JH, Keccak and Skein," ECRYPT II Hash Workshop 2011, May 2011.
- A. Maiti, P. Schaumont, "Improved Ring Oscillator PUF: An FPGA-Friendly Secure Primitive," *IACR Journal of Cryptology*, special issue on Secure Hardware, 24(2), April 2011.
- K. V. Stefanik, J. C. Gassaway, K. B. Kochersberger, and A. L. Abbott, “UAV-based Stereo Vision for Rapid Aerial Terrain Mapping,” *GIScience & Remote Sensing*, vol. 48, no. 1, 2011, pp. 24–49.
- K. E. Hoyle, N. J. Short, M. S. Hsiao, A. L. Abbott, and E. A. Fox, “Minutiae + Friction Ridges = Triplet-Based Features for Determining Sufficiency in Fingerprints,” Proceedings: 4th International Conference on Imaging for Crime Detection and Prevention (ICDP-11), London, UK, Nov. 2011.
- N. J. Short, A. L. Abbott, M. S. Hsiao, and E. A. Fox, “Latent Fingerprint Segmentation using Ridge Template Correlation,” Proceedings: 4th International Conference on Imaging for Crime Detection and Prevention (ICDP-11), London, UK, Nov. 2011.
- S. H. Park, J. P. Leidig, L. T. Li, E. A. Fox, N. J. Short, K. E. Hoyle, A. L. Abbott, and M. S. Hsiao, “Experiment and Analysis Services in a Fingerprint Digital Library for Collaborative Research,” Proceedings: International Conference on Theory and Practice of Digital Libraries (TPDL 2011), Berlin, Sept. 2011. Also in *Lecture Notes in Computer Science (LNCS),* vol. 6966, *Research and Advanced Technology for Digital Libraries*, pp. 179-191, 2011.
- P. L. Fanto, J. C. Gassaway, K. B. Kochersberger, and A. L. Abbott, “3D Mapping Techniques using a Stereo Boom on Low-Flying Vehicles,” to appear in Proceedings: ASPRS 2012 Annual Conference, Sacremento, CA, March 2012.

Books Published



- S. Ahuja, A. Lakshminarayana, and S. K. Shukla, *Low Power Design with High-Level Power Estimation and Power-Aware Synthesis*, Springer, Boston, MA, 2011, Pages. 200, Hardbound, ISBN: 978-1-4614-0871-0

Book Chapters

- J. Park and K. Bian, "Security of Cognitive Radios," in *Encyclopedia of Cryptography and Security*, Second Edition, Henk C. A. van Tilborg and Sushil Jajodia (Eds.), Springer, 2011.
- Yi. Deng, Hua Lin*, Arun Phadke, Sandeep Shukla, and Jim Thorp, “Networking Technologies for Wide Area Measurement Applications”, to be published in the *Handbook of Power Systems Engineering*, CRC press, 2011.
- L. Fang and M. S. Hsiao, "A Fast Approximation Algorithm for MIN-ONE SAT and Its Application on MAX-SAT Solving," book chapter in *Advanced Techniques in Logic Synthesis, Optimizations and Applications*, edited by Sunil P. Khatri and Kanupriya Gulati, Springer, pp. 149-170, 2011.

- H. Jagadeesan and M. S. Hsiao, "Continuous Authentication in Computers," book chapter in *Continuous Authentication Using Biometrics: Data, Models, and Metrics*, edited by Issa Traore and Ahmed Awad E. Ahmed, IGI Global, pp. 40-66, 2011.
- P. Schaumont, Z. Chen, "Side-channel Attacks and Countermeasures for Embedded Microcontrollers," in Introduction to Hardware Security and Trust, Eds M. Tehranipoor, C. Wang, 263-282, Springer.

Editors of Conference Proceedings

- Sandeep Shukla and Philippe Coussey, *International Symposim on ESL Synthesis* (ESL-syn 2011), ECSI and IEEE Computer Society Press, June 2011.
- Sandeep Shukla and Zeljko Zilic, *Proceedings of the IEEE Workshop on High Level Synthesis*, November, June 2011.
- Patrick Schaumont and Ramesh Karri, *IEEE Symposium on Hardware Oriented Security and Trust (HOST 2011), June 2011.*

Guest Editorials and Prefaces

- Shukla, Sandeep K.; Talpin, Jean-Pierre; , "Guest Editors' Introduction: Special Section on Science of Design for Safety Critical Systems," *Computers, IEEE Transactions on* , vol.60, no.8, pp.1057-1058, Aug. 2011
- Zilic, Z.; Mishra, P.; Shukla, S.; , "Challenges of Rapidly Emerging Consumer Space Multiprocessors," *Design & Test of Computers, IEEE* , vol.28, no.3, pp.52-53, May-June 2011
- Mishra, Prabhat; Zilic, Zeljko; Shukla, Sandeep; , "Guest Editors' Introduction: Multicore SoC Validation with Transaction-Level Models," *Design & Test of Computers, IEEE* , vol.28, no.3, pp.6-9, May-June 2011
- Shukla, S.; Mishra, P.; Zilic, Z.; , "A Brief History of Multiprocessors and EDA," *Design & Test of Computers, IEEE* , vol.28, no.3, pp.96, May-June 2011

Invited Presentations

- Jerry (Jung-Min) Park gave an invited presentation at the University of Texas at Arlington in April, 2011. The title of the talk was "Trustworthy cognitive radio networks". Park discussed a number of security issues relevant to dynamic spectrum access and cognitive radio networks, including regulation of transmission behavior via policy enforcement, vulnerability of cognitive radio control channels, tamper resistance of software defined radio's software, and attacks against cognitive engines.
- Sandeep Shukla, Security and Software Engineering Research Center (S2ERC) 25th year Celebration Showcase invited talk, Muncie, Indiana, May 2011, “Complex Network Approach to Software Analysis”.
- Sandeep Shukla, Office of the Secretary of Defense, Software Producibility Programme’s yearly review, Arlington, VA, November 2010, “Behavioral Types for Compatibility Checking of Software Components”, Annual Review Presentation.
- Sandeep Shukla, Office of the Secretary of Defense, Software Producibility Programme’s mid year review, Rome, NY, May 2011, “Behavioral Types for Compatibility Checking of Software Components: Status Report”, Mid-Year Review Presentation.
- Sandeep Shukla, Indraprasth Institute of Information Technology, New Delhi (IIIT-D), Invited Talk, January 2012, “Abstract Interpretation, Polychrony, and Correct-by-Construction Software Synthesis”.
- Sandeep Shukla, Indian Statistical Institute, Kolkata (ISI), Invited Talk, January 2012, “Abstract Interpretation, Polychrony, and Correct-by Construction Software Synthesis.

- Sandeep Shukla, Invited Speaker at the IEEE Recent Trends in Information Systems (ReTiS'12), Kolkata, January 2012, "Safety Critical Embedded Software Synthesis from Formal Models".
- Sandeep Shukla also also one of the panelists for a panel on System Level Verification at the ACM/IEEE Design Automation Conference (DAC 2012), San Diego, June 2011.
- Sandeep Shukla, Invited talk at NIKSUN World Wide Security & Mobility Conference, "Smart Grid: From the perspective of Cyber Security, Vulnerabilities and Countermeasures", Princeton, NJ, January 2012.
- Abhranil Maiti, Invited presentation at the NIST Workshop on Cryptography for Emerging Technologies and Applications, "A Framework for the Evaluation of Physical Unclonable Functions," Gaithersburg, 11/7/2011.
- Patrick Schaumont, Invited presentation at ESAT/COSIC (KUL), "Moving PUFs out of the lab," Leuven, Belgium, February 2012.
- Patrick Schaumont, Invited presentation at ECE Department of University of Connecticut, "Building Better Hardware for the Elliptic Curve Discrete Logarithm Problem," Storrs, CT, February 2012.