2024 IEEE Microelectronics Design and Test Symposium

May 13 through May 15, 2024, at the Desmond Crowne Plaza located in Albany, New York

The 33rd IEEE Microelectronics Design & Test Symposium (MDTS, formerly known as NATW) provides an annual world forum for academia and industry. University faculty, student researchers, and industry engineers discuss latest advances in microelectronics, share their visions in modern microelectronic technologies, and foster academy-industry collaboration. The three-day symposium features keynote, invited talks, a panel and tutorial on the themes of **chiplets** and **hardware security**. Chiplets break large chip designs into smaller, ideally reusable, integrated circuits, and the Universal Chiplet Interconnect Express (UCIe) standard addresses the challenges of connecting chiplets in the package. Hardware security for chip designs covers a broad range of issues, from preventing reverse engineering to blocking takeovers and data theft or manipulation.

MDTS 2024 is sponsored by IEEE Schenectady Section and IEEE Region 1, and is supported by Advantest Corporation, AdamsIP, Cadence Design Systems, Green Mountain Semiconductor, IBM Corporation, and co-promotion with the SWTest Conference.

Monday, May 13

11:00 am - 8:00 pm Registration (Fort Orange)

12:00 pm - 1:00 pm Lunch (Koi Pond)

1:00 pm – 5:40 pm MDTS Sessions (Shaker Room)

1:00 pm – 1:10pm **Welcome Address: Kelly Ockunzzi General Chair**

Invited Speaker

1:10 pm – 1:15 pm Speaker Introduction: Krishna Chakravardula, Cadence

1:15 pm – 2:15 pm Speaker: Aydin Aysu

Title: Emerging Security Challenges at the Junction of AI and Hardware

Abstract: While AI helps automating and improving certain classification/regression tasks, side-channel analysis allows extracting secret information from hardware that is mathematically secure. Although these were two fairly distinct research domains, they have recently been getting closer. Yet it is unclear how they would couple. In this talk, I will explain my research group's efforts on the emerging security challenges at the intersection of AI and hardware using side-channels as a driving motivation. I will first demonstrate new side-channel attacks on AI hardware that can steal valuable machine-learning models and methods for protection. Then, I will show the use of novel learning techniques to outperform classical side-channel attacks and break cryptographic systems that cannot be broken with classical attacks.

Biography: Dr. Aysu is currently an assistant professor and Bennett Faculty Fellow at the Electrical and Computer Engineering Department of North Carolina State University, where he leads HECTOR: Hardware Cybersecurity Research Lab. He got his M.S from Sabanci University in Istanbul, Turkey, and his Ph.D. from Virginia Tech. Before joining NC State, he was a post-doctoral researcher at the University of Texas at Austin. Dr. Aysu's interests are broadly in hardware security research and cybersecurity education. His hardware security research has won NSF CAREER, NSF CRII, Google RSP, and Goodnight Innovation Fellow awards, six best paper nominations (IACR TCHES, IEEE HOST, DATE, GLS-VLSI), two best paper awards, one hardware security top picks (IEEE CEDA), and one publicity paper award (DAC). He is an IEEE senior member.

Tutorial 2:15 - 5:40 PM : Chiplets and Hardware Security

2:15 pm – 2:20 pm Tutorialist Introduction: : Krishna Chakravardula, Cadence

2:20 pm – 3:20 pm Speaker: Martin Cochet

Title: Everything you always wanted to know about UCIe

Abstract: With the physical die sizes reaching their limits, many companies have been turning to partition their designs into multiple chiplets co-assembled within a package. This paves the way for multi-vendor integration and chiplets reuse across projects. To enable such an ecosystem, the UCIe consortium has recently proposed a new standard: Universal Chiplet Interconnect Express. This standard offers state-of-the art bandwidth and energy efficiency for chiplet-to-chiplet communication (>1Tb/s/mm at 0.3pJ/bit). This talk will first cover the motivations driving chipletized designs to provide both design scalability and reuse. Then I will give an overview of the full UCIe stack including protocol layer, physical IP and packaging. UCIe requires a much tighter integration between

the link, chip and package design than longer reach interconnects. Hence we will highlight the importance of understanding the interactions across those layers both for designers and users of UCIe links.
Biography: Dr. Martin Cochet is a Senior Research Scientist with the IBM Thomas J. Watson Research Center, Yorktown Heights, NY, USA. He received the Dipl.Ing. degree from the École Polytechnique, Palaiseau, France, M.S. degree from Imperial College London, U.K. and Ph.D. degree in electronic engineering from Aix-Marseille University, France in 2012, 2013 and 2016 respectively. He was previously a visiting scholar with the University of California at Berkeley, USA and a research engineer with STMicroelectronics, Crolles, France. His research interests include mixed-signal circuit design for high-speed wireline communications and digital techniques for SoC power management. He serves on the Technical Program Committee of the European Solid-State Circuit Conference.

3:20 pm – 3:30 pm Break (Beverage Service 2 - 3:30pm, Shaker Room)

3:30 pm – 3:35 pm Tutorialist Introduction: : Krishna Chakravardula, Cadence

3:35 pm – 4:35 pm Speaker: Ramesh Karri
Title: High-Level Approaches to Hardware and Embedded Security
Abstract: As designers increasingly rely on third-party intellectual property (IP) cores and outsourcing in the integrated circuit (IC) design and manufacturing process, security vulnerabilities have been on the rise. This has forced both IC designers and end users to re-evaluate their trust in ICs, as unprotected ICs are susceptible to reverse engineering, IP piracy, and the insertion of malicious circuits and backdoors. In this talk, I will present High-Level Design for Trust techniques that my group has developed to address these threats: Locking of Designs and Secure Sourcing of IPs for High-Level Integration. Implementing built-in locking mechanisms aims to prevent reverse engineering. Secure Sourcing thwarts Trojan insertion in third-party IPs. I will wrap up the presentation by emphasizing the importance of hardware security from economic, security, and safety standpoints, and share my vision for the exciting field of hardware cybersecurity.
Biography: Ramesh Karri is a Professor of Electrical and Computer Engineering at New York University. He co-directs the NYU Center for Cyber Security (http://cyber.nyu.edu). He co-founded the Trust-Hub (http://trust-hub.org) and founded/organizes the Embedded Systems Challenge (https://csaw.engineering.nyu.edu/esc), the annual red-blue team event. Ramesh Karri holds a Ph.D. in Computer Science and Engineering from the University of California at San Diego, and a B.E in ECE from Andhra University. With a focus on hardware cybersecurity, his research and educational endeavors encompass trustworthy ICs, processors, and cyber-physical systems; security-aware computer-aided design, test, verification, validation, and reliability; nano meets security; hardware security competitions, benchmarks, and metrics; biochip security; and additive manufacturing security. Ramesh has published over 300 articles in prestigious journals and conferences. A Fellow of IEEE, Ramesh's work on hardware cybersecurity has earned numerous best paper award nominations (ICCD 2015 and DFTS 2015) and awards (ITC 2014, CCS 2013, DFTS 2013, VLSI Design 2012, ACM Student Research Competition at DAC 2012, ICCAD 2013, DAC 2014, ACM Grand Finals 2013, Kaspersky Challenge, and Embedded Security Challenge). He has also received the Humboldt Fellowship and the National Science Foundation CAREER Award. Ramesh is the Editor in Chief of the ACM Journal of Emerging Computing Technologies and an Associate Editor for IEEE and ACM journals. He's had leadership roles in various IEEE conferences like ICCD, HOST, DFTS, and others. He served as an IEEE Computer Society Distinguished Visitor from 2013-2015 and was on the Executive Committee for Security@DAC from 2014-2017. Additionally, he's been on multiple PCs and delivered keynotes on Hardware Security and Trust at events like ESRF, DAC, MICRO.

4:35 pm – 4:40 pm Tutorialist Introduction: : Krishna Chakravardula, Cadence

4:40 pm – 5:25 pm Speaker: Paul Reuter
Title: IEEE P3405 Introduction, status update (Chiplet interconnect test and repair)
Abstract: IEEE P3405 is a working group studying the problem of chiplet interconnect test and repair. This working group is intending to develop an IEEE standard that will work with existing IEEE standards and provide a method such that chiplets provided by different companies and developed using different EDA tools can be integrated into one package and have an automated solution to test and repair the chiplet interconnect.
IEEE P3405 is a recently formed working group, and we are still gathering data and setting the scope of this standard. This presentation is an overview of the information that has been discussed so far and the many questions that remain in order to set the scope and main purpose of this standard.
Biography: Paul has a BS from the University of Cincinnati in Electrical Engineering, and a Masters in Theology from Anna Maria College. Paul has worked for Siemens (formerly Mentor Graphics) since 1996, working on developing industry leading DFT EDA tools. Prior to this he worked at Digital Equipment Corp for 12 years. He has been active in IEEE standards working groups, participating in IEEE 1450.0, 1450.1, 1450.6, 1687, P3405 and

others. He is co-inventor on five US patents and has presented papers at ITC and NATW (MDTS) and past General Chair of NATW.
6:00 pm – 7:30 pm Opening Reception Dinner Buffet (Koi Pond)
7:30 pm – 9:00 pm **Panel: "Rise of the Chiplets" - Design, Test and Hardware Security**
Panel Chair: Malinky Ghosh Panel Moderator: Eugene Atwood
Panelists
Ramesh Karri, Professor, Electrical and Computer Engineering, New York University
Martin Cochet, Senior Research Scientist, IBM Research
Nathaniel Cady, Associate Dean, University at Albany, The State University of New York
Paul Reuter, Senior Software Engineer, Siemens Digital Industries Software

Tuesday, May 14

7:00 am - 6:00 pm Registration (Fort Orange)

7:00 am - 8:30 am Breakfast (food service 7-8:30am, Shaker Room)

8:30 am – 6:40 pm MDTS Sessions (Shaker Room)

Session 1

8:30 am - 8:35 am Welcome: Kelly Ockunzzi General Chair

8:35 am – 8:45 am Program Introduction: Uma Srinivasan Program Chair

Invited Speaker

8:45 am – 8:50 am **Invited Speaker** Introduction: Tian Xia, University of Vermont

8:50 am – 9:50 am Invited Speaker: John Oakley

Title: SRC's Microelectronics and Advanced Packaging Technologies (MAPT) Roadmap: Driving a New Era of Innovation in Semiconductors and Digital Twins

Abstract: The semiconductor industry is on the brink of a new era of innovation, propelled by the convergence of Microelectronics and Advanced Packaging Technologies (MAPT). This talk explores how the Semiconductor Research Corporation (SRC) is spearheading this transformation by democratizing and accelerating innovation in research, design, and manufacturing. Central to this initiative is the development of a Digital Twin Platform/Framework (DT backbone) that serves as the foundation for collaborative endeavors. This framework will ensure data and tool accessibility across all members while prioritizing secure management protocols. SRC is fostering an ecosystem where members can engage and exchange ideas, collaborate on project proposals, conduct privately funded projects, access funding opportunities, and test Digital Twin innovations. An integral aspect of SRC's MAPT Roadmap is the emphasis on attracting and training a workforce equipped to harness the potential of Digital Twins. By integrating Digital Twin technologies into education and training programs, SRC ensures a pipeline of talent capable of driving innovation forward. Ultimately, SRC's MAPT roadmap is not only about conceptualization but also about delivery. By seamlessly integrating Digital Twin innovations into the manufacturing value chain, SRC is paving the way for a future where semiconductor advancements are not only envisioned but also realized.

Biography: John Oakley, a Science Director at SRC, is focused on leading several collaborative research programs including Hardware Security (HWS), Packaging (PKG), AI Hardware (AIHW), and Supply Chain AI Realized Future (SCARF). John works closely with government, industry, and university partners to advance these research topics. Through this work John has created and managed research programs in collaboration with industry, government, and academia. John also serves as a Board member of the Florida Institute for Cybersecurity Research (FICS). A graduate of Texas A&M University, John has over 20 years of successful digital design and architecture experience in industry and was formerly a RF Control Architect at Intel Corporation, at Motorola, Freescale, Fujitsu. John has 14 issued patents and has developed more than 55 successful integrated devices, several of which have shipped in high volumes. He has worked in numerous digital system spaces and was focused on the transceiver and modem fields and on the control planes of cellular platforms.

Student Paper Session 1 & 2

Session Chair: : Tian Xia, University of Vermont

9:50 am - 10:10 am Paper 1.1:
Title: Integrating ReRAM for Neuromorphic Computing: Real-time testing of packaged 64x64 1T1R crossbar arrays using a custom build microcontroller board
Author: Jeelka Natwarbhai Solanki (University at Albany)
Abstract: Neuromorphic systems hold potential for overcoming conventional computing limitations by executing compute operations in or near memory. Computation-in-memory, employing innovative synaptic devices like memristors, aims to alleviate the von Neumann bottleneck by performing multiply and accumulate (MAC) operations within resistive memory arrays. Resistive random access memory (ReRAM), a type of memristive device, can be switched between high and low resistance states, facilitating current flow modulation through applied voltage. ReRAM, including the 1 transistor-1 ReRAM (1T1R) cell configuration, supports analog memory and mimics neural synapses, promising efficient calculations with low energy consumption. Our team at the University at Albany and NY CREATES has developed Hafnium oxide (HfOx) based CMOS integrated ReRAM, including individual 1T1R cells and memory arrays up to 64 x 64 1T1R, using 65nm technology. To enable precise matrix-based computing within 1T1R ReRAM arrays, a custom circuit board integrated with a Nuvoton microcontroller was designed and fabricated. The board addresses parameters such as fast programming pulse fast (1us) delivery, variable voltage application(-5 V to +5 V), and accurate current (nA-mA) or resistance(Kohm) measurement. During vector matrix multiplication (VMM) operations, distinct output currents from columns differentiate between unique inputs applied to rows, enabling various applications including convolutional neural networks (CNNs) and deep learning networks. The board's current focus is on demonstrating a robotic application designed for line tracking, with future plans to extend functionality to image comparison tasks using convolutional neural networks. This hardware facilitates in-memory computing operations with low energy usage, showcasing the potential of ReRAM in overcoming traditional computing constraints.
Biography: Jeelka graduated with a master's degree from The Maharaja Sayajirao University of Baroda, Gujarat, India specializing in Embedded systems with hardware design and software programming in 2015. Her undergraduate research was majorly in designing a hardware based on microcontroller for bag making machine in the field of Electronics and Communications. She is currently pursuing her PhD in Nanoscale science and Engineering. With her constant interest and experience in designing hardware and software programming, she is working on designing hardware for programming RRAM devices in the packaged form building a bridge between characterization and real-world applications like Artificial Intelligence & Machine Learning. Jeelka has active research interests in the latest non-volatile memory technology namely RRAM and its in-memory computing techniques which demonstrates neuromorphic computing.

10:10 am – 10:25 am Break (Beverage Service 10 - 11:30am, Shaker Room)

10:25 am - 10:45 am Paper 1.2: (Remote)
Title: Design of an OTA circuit for low voltage applications
Author: Prasanta K. Ghosh (Syracuse University), Pushkar Mishra (Syracuse University)
Abstract: Literatures show clear preference of n-channel metal oxide semiconductor for the design of operational transconductance amplifier (OTA). There are advantages in using NMOS, but at the same time there are limitations especially in designing circuit for medical applications. Reported threshold voltage of 180nm device is around 400 mV, making these devices restrictive for low-voltage applications such as for ECG machine. An alternative approach to make these devices useful for low voltage applications would be utilization of the fourth terminal of the MOS device to optimize the voltage headroom. Bulk terminal needs lesser voltage source than the gate-driven transistors. It should be noted that the bulk-driven input stage ensures the amplification in the subthreshold region. Additionally, a rail-to-rail input stage is employed to improve the leakage current. Attentional has also be given to fluctuations in open loop gain due to the change in input signal. Design shows that addition of a second stage for the OTA using a compensation technique helps improve the circuit response. It reduces impact of intrinsic transconductance on the total open loop gain of the amplifier. Furthermore, adding a second stage improves the gain by distributing the dependency of the gain on both poles in the circuit. Hence, the problem of fluctuating transconductance of the input stage is resolved by the constant intrinsic transconductance of the MOS near the second pole. Design includes a 180nm Operational Transconductance Amplifier circuit with improved open loop gain with a 0.9V supply voltage. Simulation results show an open loop gain of 97.14 dB with a power consumption of 3.33uW. These results clearly show its potential for low-voltage applications. The slew rate of the OTA is 0.05V/μS with a unity-gain bandwidth of 8.4MHz. The gain-bandwidth product of this design is optimized to ensure minimum deviation of total open loop gain with respect to the changing input signal.
Biography: Pushkar Nath Mishra is an accomplished Electrical Engineer with a master's degree in electrical engineering from Syracuse University, currently aspiring to pursue a PhD in the same field. With a strong foundation in theoretical and practical aspects of electrical engineering, his expertise spans Analog Circuit Design,

memory computing, and a wide array of relevant technologies. Pushkar's professional journey includes a significant stint as a Research Assistant at Syracuse University, where he made substantial contributions to biomedical signal processing through his work on Operational Transconductance Amplifiers. He also has industry experience as an Analog Design Engineer at NXP Semiconductor Pvt Ltd in Bangalore, India, where he was involved in view verification, MOS-Bitcell Analysis, and optimization projects for various memory components. As an educator, he was a Teaching Assistant, facilitating hands-on learning and ensuring students' thorough understanding of circuit design principles. Pushkar has undertaken various projects, from developing high-gain OTAs for low-voltage applications to creating autonomous vehicles and air quality monitoring systems. His technical proficiency is further evidenced by his adeptness with EDA tools, programming languages, and lab equipment. Pushkar is committed to advancing his knowledge and aims to contribute innovative solutions to the engineering community, as show cased by his diverse academic and professional experiences.

10:45 am - 11:05 am Paper 1.3
Title: Harmonic Tag with Probe-Fed Patch Antennas
Author: Swarup Chakraborty (University of Vermont)
Abstract: This paper presents a multi-layer passive harmonic tag design. The tag is made of three layers: the top layer features the antenna units, the second layer consists of a plain ground surface, and the bottom layer houses a Schottky diode and impedance-matching circuit operating within this framework.
Biography: Swarup Chakraborty is a Ph.D. student with the Department of Electrical and Biomedical Engineering, University of Vermont. His research interest is in radio frequency circuit design and characterization.

Paper Session 2

Session Chair: : Paul Reuter, Siemens

11:05 am – 11:25 am: Paper 2.1
Title: Within-Chip Bridged-Pattern Short Detection Using Spatially Distributed Kerf Test Structures in 7nm FinFET Technology
Author: Cheng-Yi Lin (International Business Machines Corp.)
Abstract: This paper presents a bridged-pattern short detection method using the composite yield of spatially distributed minimum pitch metal kerf test structures to capture within-chip non-uniform yield variation. Location and layout analyses reveal a top-to-bottom yield delta within the product chip and a correlation to the metal tip-to-side shorting monitors, suggesting a bridged-pattern short. An inline scan chain latch macro also detects this signature with better signal strength. These inline monitors can unveil a within-chip bridged-pattern short defect when spatially distributed. They provide area-efficient early detection of this defect mode.
Biography: Mr. Lin started his career at IBM Systems in 2015. He is an Advisory Power Product Characterization Engineer, and he works on the 7HPP technology to drive the delivery of high-performance P10 server chips. His expertise includes data analysis/mining of in-line electrical signals, product yield, and Wafer Final Test (WFT) results. To drive manufacturing improvement, he provided root cause analysis of Health of Line (HOL) macros, functional yields, and device parameter metrics with vintage, tool/chamber understanding. In addition, he established WFT comments, performed data visualization, conducted correlation studies, investigated lot history, and provided yield projections to support production and process controls. With gratitude, his corporate honors included Manager Choice Award and Cultural Catalyst Award. Before joining IBM, he was a Research Assistant in the Duan and Device Research Laboratory at UCLA. He prototyped and optimized a portable, internet-capable, low-cost readout circuit for In2O3/RGO nanocomposite gas sensors. In 2008, he was a Summer Intern in the Process Integration Engineering Department of Taiwan Semiconductor Manufacturing Company (TSMC) in Hsinchu, Taiwan. He optimized halo implant conditions via TCAD simulation for 35HV 13.5V PMOS in 0.35 μm technology. Mr. Lin received his M.S. degree in Electrical Engineering (EE) from the University of California, Los Angeles (UCLA), his B.S. degree in Power Mechanical Engineering, and an M.S. degree in Electronic Engineering from National Tsing-Hua University (NTHU) in Hsinchu, Taiwan. Besides, he was awarded a Government Scholarship to Study Abroad from the Ministry of Education, Taiwan. He has published three technical papers, a patent, several publications through IBM, and conducted numerous EE projects. Also, he was selected as an Honorary Member of Talent Net—Epoch Foundation in 2009 and is an IEEE member.

11:25 pm - 11:45 pm Paper 2.2:
Title: On the Design of a 20 Channel Pin Parametric Measurement System for Post-Fabrication Testing
Author: Xiaozhe Fan (GlobalFoundries)
Abstract: A new era of consumer electronics has arrived asa result of significant advancements in Artificial intelligence (AI) and Internet of Things (IoT) applications. In order to secure long-term and stable operations of an integrated circuit(IC), parametric measurements have been one of must-have test procedures for post-fabrication

production testing. This paper presents a 20 channel pin parametric measurement system, capable of performing four-quadrature parametric measurements. The system was built using off-the-shelf hardware components. As a proof of concept, the proposed system was verified in Force Voltage (FV) mode with the aid of an external digital multimeter (DMM). Besides, a simplified linear regression (SLR) method was employed to calibrate the proposed system. Calibration results have shown that PMU FV errors undergo a reduction of more than 400 times while using the SLR-based calibration method

Biography: Xiaozhe Fan was born in Taiyuan, China, in 1990. He received the B.Sc. degree in electrical engineering from the Tianjin University of Science and Technology, in June 2013, and the Ph.D. degree in electrical engineering technology from Purdue University, in 2021. He is currently working as a Principal Test Development Engineer in GlobalFoundries.

12:00 pm - 1:00 pm Lunch (Koi Pond)

1:00 pm – 1:05 pm **Invited Speaker** Introduction: Paul Reuter, Siemens

1:05 pm – 2:05 pm Invited Speaker: Gordon Harling

Title: Platforms for Creating and Integrating Chiplets

Abstract: There is value in integrating commercial-off-the-shelf components from various technologies into the same package or module but even greater product differentiation and performance can be achieved when chiplets can be inexpensively modified to suit a particular purpose. In this paper we discuss open source designs which can be prototyped using a cost-effective and low risk prototyping service. They can then be integrated using custom LTCC modules or silicon interposers.

Biography: Gordon Harling received a Bachelor's degree in Applied Science from the University of Toronto and a Maitrise en Ingenierie Physique from the Ecole Polytechnique de Montreal. He has worked in Research and Development at large companies such as Mitel, NovAtel, and DALSA. He has been a founder and CEO of several start-up companies including Goal Semiconductor, Elliptic Technologies, and Innotime Technologies. He is CEO of CMC Microsystems, a not-for-profit which provides software and services to small and medium enterprises and assists over 10 000 researchers and students in over 80 colleges and universities across Canada, the USA, Mexico, and Australia.tch:

2:05 pm – 2:10 pm: **Invited Speaker**: Introduction: Paul Reuter, Siemens

2:10 pm – 3:10 pm: Invited Speaker: Selçuk Köse

Title: Side-channel Leakage in Superconducting Electronics: Foe or Friend?

Abstract: Superconducting digital electronics is a promising candidate for energy-efficient high-performance computing applications such as data centers and cloud computing. Additionally, it can be used in a large-scale in-fridge qubit control and readout circuitry of superconducting quantum computers. In recent studies, a substantial power side-channel leakage has been uncovered in the superconducting interface circuits that is in the order of tens of microamperes. This leakage makes the superconducting classical and quantum computing systems vulnerable to various side-channel attacks. In this talk, potential threat models and attack scenarios will be discussed. Besides using the side-channel leakage for malicious purposes, we will present an alternative perspective, where the leakage information is used for cryogenic testing and verification of superconducting digital chips. Possible advantages and challenges of such type of testing will be discussed.

Biography: Selçuk Köse is an Associate Professor in the Department of Electrical and Computer Engineering, University of Rochester, Rochester. He received NSF CAREER award (2014), USF College of Engineering Outstanding Junior Research Achievement Award (2014), USF Outstanding Faculty Award (2016), Cisco Research Award (2015, 2016 & 2017) and USF Outstanding Research Achievement Award (2017). He has served as an associate editor for IEEE Transactions on Circuits and Systems I: Regular Papers (TCAS-1), Springer Nature-Computer Science, and Microelectronics Journal. His current research interests include hardware security with a specific focus on side-channel attacks, fault injection attacks, covert channel attacks, individual and combined countermeasures, physically unclonable functions, and true random number generators; the analysis and design of high performance/low power integrated circuits; on-chip reconfigurable DC-DC converters; interconnect related issues with a specific emphasis on the design and analysis of power and clock distribution networks; 2.5D and 3-D heterogeneous integration; emerging transistor technologies with a specific focus on graphene nanoribbon field effect transistor (GNRFET); and cryogenic electronics with a specific focus on quantum-classical interface. His research is currently supported by National Science Foundation (NSF), Semiconductor Research Corporation (SRC), Defense Advanced Research Projects Agency (DARPA), and Department of Energy (DoE).

3:10 – 3:40 pm Break (Beverage Service 2 - 3:30pm, Shaker Room)

3:40pm – 5:40pm Albany Nanotech Tour

6:30 pm – 8:30 pm: Dinner and Recognition Event: Best Student Paper Award

Wednesday, May 15

7:00 am – 11:00 am Registration (Fort Orange)

7:00 am – 8:00 am Breakfast (food service 7-8:30am, Shaker Room)

8:00 am – 12:00 pm MDTS Sessions (Shaker Room)

8:00 am - 8:05 am Welcome: Kelly Ockunzzi General Chair

Invited Speaker

8:05 am – 8:10 am: Invited Speaker: Introduction: Eric Hunt-Schroeder

8:10 am – 9:05 am: Invited Speaker: Dean Sullivan

Title: "To break it, or fix it, that is the question"

Abstract: There has recently been an explosion of attacks targeting a range of computing systems, from low-end embedded edge devices to HPC clusters. Secure solutions are then reactively deployed to combat these threats as they arise. However, a secure system is only as robust as its weakest component and, what's more, emergent threats repeatedly undermine these "secure-by-design" solutions. Rather than seeking to defend against these threats with piecemeal or ad-hoc solutions, effort should instead focus on incorporating vulnerability discovery into the design life-cycle. The goal of this talk will be not only to survey emerging attacks and attack surfaces over a range of application domains, but also methods for their automatic discovery in an effort to highlight its importance.

Biography: Dean Sullivan is an assistant professor in the Electrical and Computer Engineering department at the University of New Hampshire, where he directs the Resilient Architecture Laboratory. His research focuses on building secure systems and spans areas of (micro)architectural security, side-channels and fault-injection, and program analysis. He received a BS degree in Electrical Engineering and MS in Computer Engineering from the University of Central Florida, and his PhD in Electrical and Computer Engineering from the University of Florida. He received best papers awards for his research at DAC'16, IEEE Security & Privacy'22, and AsianHost'23.

Paper Session 3

Session Chair : Eric Hunt-Schroeder

9:05 am – 9:25 am: Paper 3.1

Title: Machine Learning Infused Software Testing for Mobile Device Development

Author: Sunder Chakravarty (Zebra Technologies Corporation)

Abstract: Automated test systems execute a large set of test cases across mobile devices that are distributed throughout the global test labs. The test cases generate a huge amount of data which consists of various logs that are captured from the mobile devices under teat and the automated test systems. The logs that are associated with the failed test cases are typically manually analyzed to determine if the failure is a true product failure or an issue with the test environment. This binary classification is performed for each test failure. The failures classified as test environment failures are further classified into subcategories. The outcome of this analysis helps ensure the test case failures are properly triaged and the respective team can take the appropriate action. Our study demonstrates the potential application of data mining techniques to automatically categorize failed test cases using the test logs. These logs contain explicit details such as time stamps, log levels, the tested module, error codes, and test outcomes. Moreover, they also have implicit information such as line velocity, error velocity, test duration, and sentiment profile. We utilize heuristics to extract both the explicit and implicit information as features. These features are associated to training labels using a subset of the logs. Our experimentation involved multiple models, including Naïve Bayes, Random Forest, Decision Tree, and Decision Table.

Biography: Head of Engineering (SW, HW, QA, Innovation, Customer support) with expertise in leading Large Global Engineering teams (300+ engineers, USA, India, China, Taiwan, Canada, Germany, Finland) expertise range from Embedded products to Cloud solutions delivering multimillion-dollar revenue generating products.
30 years of Retail industry, Telecommunication, Embedded and Application Product development (Lucent, Motorola, Nokia, Zebra)

9:25 am – 9:45 am Paper 3.2

Title: Co-design of a Novel Highly Parallel Multi-Thousand Multi-Chip Neural Network Accelerator in 28nm CMOS

Author: Ewan McNeil (Green Mountain Semiconductor)

Abstract: We are presenting a prototype AI processor with over 3000 cores for image and pattern recognition at the edge. The architecture showcases a successful codevelopment effort negotiating between software/algorithm based conceptual ideas and VLSI design realities. A digital twin of the proposed hardware was developed early on

to ensure that the technical implementation met the needs of the software team, and was maintained throughout the project. Special consideration was given to power consumption, resulting in an innovative communication protocol which minimizes power. Data transport costs between nodes were cut in half by eliminating the address bus through local target address matching. High level coding of the entire chip made it possible to quickly respond to change
requests from the software team, and to feed back the hardware implementation in real time for joint verification. This sped up the development process and improved the overall outcome, as the software team was able to continue to innovate alongside the circuit design team's implementation effort with little impact on the overall schedule. Preliminary test data is also being presented herein.
Biography: Ewan McNeil is an Electrical Engineer with Green Mountain Semiconductor. Ewan received a Bachelors from Concordia University in Montreal, Ewan is currently based in Burlington Vermont. Ewan's interests include Analog Design and Neuromorphic computing. Previous experience includes Design of a Phase Locked Loop, Operational Amplifiers and Voltage references. Implementing interfaces for communication protocols such as LPDDR5 and Technical writing for Small Business Innovation Research (SBIR) Proposals**.**

9:45 am – 10:05 am: Paper 3.3
Title: Gate Resistance Test Structures Bounded by Local Layout Density to Characterize Metal Gate Height Variation in 7nm FinFET Technology
Author: Justin Zhu (International Business Machines)
Abstract: Metal gate height (MGH) control is a critical mission in 7nm FinFET process. Gate lateral resistance, usually measured on a four-terminal test structure, is a convenient indicator of gate height. This abstract demonstrates the successful application of a set of gate resistance test structures with various local gate densities that discovered MGH variability systematics as a yield detractor in chip products, facilitated process improvement, and guided chip design optimization. They also exemplify effective process monitors that stay relevant to the context of product design.
Biography: Justin joined IBM Systems (now IBM Infrastructure) in 2018. He previously worked at Global Foundries in Malta, NY after earning PhD in Materials Science & Technology from the University of Pennsylvania in 2015 and BS in Physics from Fudan University in 2009.

10:05 am - 10:15 am Break (Beverage Service 10 - 11:30am, Shaker Room)

Paper Session 4

Session Chair: Eric Hunt-Schroeder

10:15 am – 10:35 am Paper 4.1
Title: Imaging Resistant Mask Programmable Read Only Memory (ROM)
Author: Eric Hunt-Schroeder (Marvell)
Abstract: Designed and manufactured in a 5-nm FinFET technology is a 256 Kb Secure Read Only Memory (ROM). Unlike a conventional ROM that stores data with a via connection, this Secure ROM uses two mismatched threshold voltage NFETs (twin-cell) to store data securely. Imaging techniques used to reverse engineer conventional via programmed ROMs will be unable to differentiate a data '0' from data '1.' Differential current sensing is used to briefly determine the data stored when sensed and maintains secure data at rest at all other times. The Secure ROM supports 0.675V to 0.960V at-circuit voltages and junction temperatures of -40°C to 125°C. A time zero (T0) test screen using a current imbalance while sensing to reduce test time and can predict early end of life failures from insufficient differential signal with natural aging effects in CMOS devices.
Biography: Eric Hunt-Schroeder is a Senior Staff Manager in the Central Engineering Foundational IP group at Marvell Technology located in Burlington, VT. He has 10 years of circuit design experience focused on memory development and hardware security. During his career at IBM, GLOBALFOUNDRIES and Marvell Eric has worked on the design and development of embedded DRAM, SRAM, charge trap transistor memories and Physical Unclonable Functions. Eric is a licensed Professional Engineer and has filed over 40 patents. He received his BSEE from the University of Vermont in 2013 and MSEE from SUNY Binghamton in 2015. Eric is currently pursuing a PhD in Electrical Engineering at the University of Vermont. His research focus is hardware security and Physical Unclonable Functions working with Dr. Tian Xia.

10:35 am – 10:55 am Paper 4.2
Title: High-Speed Receiver Transient Modeling with Generative Adversarial Networks
Author: Priyank Kashyap (Hewlett-Packard Enterprise)
Abstract: Data-intensive applications such as artificial intelligence and graph processing are becoming commonplace, requiring high-speed IO to enable the deployment of these critical applications. To accommodate the increasing data requirements Serializer/Deserializer (SerDes) receivers have become increasingly complex, with

different equalization schemes to mitigate channel impairments. It has become increasingly important to model this receiver as they are performance-critical.
This paper shows an approach to modeling the transient of a high-speed receiver with fixed and varying equalization through generative networks. The method considers the receiver as a black box, with its inputs and outputs as two different domains, framing the problem as a domain translation task. The proposed approach uses an intermediate representation of the time series to model the receiver successfully. We demonstrate that the proposed method is invariant to the input waveform, receiver configuration, and channel. In a fixed equalization setting, the proposed approach has a root mean squared error of 0.016 in a [0,1] range and an error of 0.054 in the same range for a variable redriver. The approach can predict a batched set of results in under 100ms, faster than an equivalent spice model for the same time steps.
Biography: Priyank Kashyap is a Hardware Engineering Specialist in the Storage Division of Hewlett-Packard Enterprise, where he works at the intersection of machine learning and signal integrity. He received his B.S. in Electrical and Computer Engineering from the New York Institute of Technology, New York, USA, in 2017 and his M.S. and Ph.D. in Computer Engineering from North Carolina State University, North Carolina, USA, in 2022 and 2023, respectively. His research interests include applying machine learning to EDA, hardware security, and quantum computing. He was the recipient of the best paper award at DesignCon 2023.

Invited Speaker

10:55 am – 11:00 am: Invited Speaker Introduction: Eric Hunt-Schroeder

11:00 am – 11:50 am: Invited Speaker: Xiaolin Xu
Title: On the Dark Side of FPGA as A Cloud-Hardware Accelerator
Abstract: The field-programmable gate arrays (FPGA) have become an emerging hardware accelerator for diverse applications. They have been integrated into the cloud-computing infrastructures by the leading cloud-service vendors like Amazon and Microsoft. However, the current studies for cloud-FPGA virtualization are predominantly focused on its performance. This talk presents several trustworthy issues associated with this emerging computing platform. Specifically, I will present several active attacks against the multi-tenant cloud-FPGA with machine learning and deep neural network as study cases. The presented attack vectors are the first of their kind, revealing a largely under-explored attack surface of using FPGA as a cloud-hardware accelerator.
Biography: Xiaolin Xu is currently an Assistant Professor with the Department of Electrical and Computer Engineering, Northeastern University. He received B.S. and M.S. degrees from the University of Electronic Science and Technology of China and his Ph.D. degree in electrical and computer engineering from the UMass Amherst. He was a Post-Doctoral Fellow with the Florida Institute for Cybersecurity Research center. His research interests span security, FPGA, computer architecture, Machine Learning, embedded system, and VLSI. His research works received the Rookie Author of the Year (RAY) Award from ACM Transactions on Design Automation of Electronic Systems (TODAES) 2022, Best Paper nomination from Embedded Systems Week (ESWEEK) 2022, and Best Paper nomination from the International Conference on Computer-Aided Design (ICCAD) 2022. He is a recipient of the National Science Foundation Early CAREER award.

11:50 am – 12:00 pm **Closing Remarks, Andrew Laidler Vice General Chair**

12:00 pm – 1:00 pm Lunch (Koi Pond)

Please complete our survey online:

Microelectronic Design and Test Symposium 2024 Survey