May 13 -15, 2024

IEEE MICROELECTRONICS DESIGN & TEST SYMPOSIUM

http://mdts.ieee.org

Tutorial Sessions: Chiplet Standards and Hardware Security

	Day 1: Monday, May 13, 2024 2:15 – 5:40 PM		
	Speaker	Affiliation	Topic
1a	Martin Cochet	IBM	Everything you always wanted to know about UCIe
1b	Ramesh Karri	New York University	High-Level Approaches to Hardware and Embedded Security
1c	Paul Reuter	Siemens DISW	IEEE P3405 Introduction, status update (Chiplet interconnect test and repair)
	Day 2: Tuesday, May 14, 2024 8:50 – 9:50 AM and 1:05 – 2:05 PM		
1a	John Oakley	SRC Semiconductor Research Corporation	Microelectronics and Advanced Packaging Technologies (MAPT) Roadmap: Driving a New Era of Innovation in Semiconductors and Digital Twins
3c	Gordon Harling	CMC Microsystems	Platforms for creating and integrating chiplets

Tutorial Session: Chiplet Standards and Hardware Security

Chiplets offer distinct physical, electronic and market-based advantages as an important and emerging advanced packaging technology. These tutorial sessions introduce design, test and hardware security aspects and present the open-source chiplet standard: UCIe (Universal Chiplet Interconnect Express) and Chiplets as part of the Advanced Packaging Roadmap from SRC (Semicoductor Research Corporation) with latest developments on the IEEE chiplet working group P3405 (Test and Repair).

Outcomes from these tutorial sessions include:

- Introduction to *UCIe (Universal Chiplet Interconnect Express)* standard (IBM)
- Recognition of *Chiplet Hardware Security* consideration for chiplets (NYU)
- Understanding *Chiplet Roadmap* assembly and integration goals (SRC)
- Updates from *Chiplet Test and Repair* (IEEE P3405 working group)
- Awareness of *Chiplet Design Platform* Concepts (CMC)

Tutorial attendance is eligible for PDH (Professional Development Hours) upon request.

Everything You Always Wanted to Know About UCIe* (*But Were Afraid to Ask)

Martin Cochet

IBM TJ. Watson Research Center,
1101 Kitchawan Road/Rte 134, Yorktown Heights, NY 10598, United States
Email: martin.cochet@ibm.com

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.

Biosketch: 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.

URL: https://research.ibm.com/labs/yorktown-heights

High-Level Approaches to Hardware and Embedded Security

Ramesh Karri

Tandon School of Engineering, Polytechnic Institute, New York University,
6 Metrotech Center, Brooklyn, NY 11201, United States
Email: rkarri@nyu.edu

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.

Biosketch: 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.

URL: http://engineering.nyu.edu/people/ramesh-karri

IEEE P3405 Introduction, Status Update (Chiplet Interconnect Test and Repair)

Paul Reuter

Siemens Digital Industries Software
300 Nickerson Rd, Suite 200, Marlboro, MA 01752, United States
Email: paul.reuter@siemens.com

Abstract: This standard defines effective and efficient mechanisms to test and repair chiplet interconnects. The standard includes the following: 1. An Architecture definition for the test and repair of chiplet interconnects. The architecture consists of the following elements: chiplet interconnect clustering, cluster clocking and redundancy, cluster repair muxing and mux re-configuration support, lane numbering and repair signature format. In addition, the standard defines testing support for high volume manufacturing of chiplet interconnects. 2. A description language that defines the test and repair hardware, the signature format, message format for communication between the two dies and the die models used for validating the test infrastructure.

Biosketch: 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.

URL:https://eda.sw.siemens.com/en-US/

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

John Oakley

Semiconductor Research Corporation, 4819 Emperor Blvd., Suite 300. Durham NC 27703, United States
Email: oakleyjohn42@gmail.com

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.

Biosketch: 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.

URL:https://src.org/about/management-team/oakley-john/

Platforms for Creating and Integrating Chiplets

Gordon Harling

CMC Microsystems, S 1111 Notre-Dame West, Pavillon B, Suite B-0710
Montreal, Quebec H3C 6M8, CA
Email: Harling@cmc.ca

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.

Biosketch: 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.

URL: https://www.cmc.ca/