

January 2023

<https://site.ieee.org/rockrivervalley/>

Rock River Valley Section

Event

Sense

The Institute of Electrical and Electronic Engineers, Inc.

IEEE RRV Section, CCS Chapter, WIE, LM and YP Affinity Group Meeting
SERVING IEEE MEMBERS OF NORTH CENTRAL ILLINOIS AND SOUTH CENTRAL WISCONSIN

WHEN Thursday, January 26, 2022

WHERE:

Webex(see Page 2)

AGENDA

7:00 pm Login

7:15 pm Presentation



Hardware Security: Functional Encryption and Chip Authentication

Dr. Keshab K. Parhi, PhD, IEEE Fellow

IEEE CCS Distinguished Lecturer

Professor, University of Minnesota, Minneapolis

This talk will present approaches to functional obfuscation where the functionality is hidden by incorporating keys to a design such that the circuit only functions correctly if the key is correct. Various modes are introduced such that only the correct key triggers the correct functionality of the chip. One goal is to prevent foundries from manufacturing excess parts and third party vendors from selling in black market. Another goal is to prevent theft of intellectual property. A third goal of obfuscation is to prevent reverse engineering. I will introduce the notions of fixed and dynamic functional obfuscation. We will show that the time to find the key by trial and error can be increased exponentially with respect to the number of key bits with dynamic obfuscation. In the second part of the talk, I will discuss chip authentication using physical unclonable functions (PUFs). These are small circuits that can exploit manufacturing process variations to generate unique signatures of chips. These unique signatures, in the form of challenge-response pairs, can be stored in a server and can be used to authenticate devices. Various delay-based PUFs include multiplexer (MUX) PUF and ring-oscillator PUF. I will talk about modeling both linear and nonlinear MUX PUFs. We will show that both hard and soft responses of linear and nonlinear MUX PUFs can be modeled by artificial neural network. I will then talk about XOR PUFs and feed-forward XOR PUFs that are more secure.

See next page for webex information

Please register online at

<https://meetings.vtools.ieee.org/m/338655>

Biography: Dr. Biography: Dr. Keshab K. Parhi received the B.Tech. degree from the Indian Institute of Technology (IIT), Kharagpur, in 1982, the M.S.E.E. degree from the University of Pennsylvania, Philadelphia, in 1984, and the Ph.D. degree from the University of California, Berkeley, in 1988. He has been with the University of Minnesota, Minneapolis, since 1988, where he is currently Erwin A. Kelen Chair in Electrical Engineering and Distinguished McKnight University Professor in the Department of Electrical and Computer Engineering. He has published over 700 papers, is the inventor of 34 patents, and has authored the textbook VLSI Digital Signal Processing Systems (John Wiley & Sons, 1999). His current research addresses VLSI architecture design of machine learning systems, hardware security, data-driven neuroscience and DNA computing. Dr. Parhi is the recipient of numerous awards including the 2017 Mac Van Valkenburg award and the 2012 Charles A. Desoer Technical Achievement award from the IEEE Circuits and Systems Society, the 2004 F. E. Terman award from the American Society of Engineering Education, and the 2003 IEEE Kiyo Tomiyasu Technical Field Award. He received the 2013 Distinguished Alumnus award from the IIT Kharagpur. He has served as the Editor-in-Chief of the IEEE Trans. Circuits and Systems, Part-I during 2004 and 2005. He is a Fellow of IEEE, ACM, AIMBE, AAAS and the National Academy of Inventors.

JOIN WEBEX MEETING:

<https://ieeemeetings.webex.com/ieeemeetings/j.php?MTID=m2a3c2ca9186f0b6418bc01581f91fb90>

Meeting number: 2536 646 3200

Password: w3GEpx7bKn3

Join by phone

+1-415-655-0002 United States Toll

1-855-282-6330 United States Toll Free

Access code: 253 664 63200

**IEEE Rock River Valley Section
2023 Officers**

Chair: Terry Johnson

Vice Chair: Alkesh Patel

Secretary: Patrick Conner

Treasurer: Adrian Vandergrift

Communications Chair: Rakesh Vasudevan

Co- Treasurer: Lawrence Wachowiak

IAS Chapter Chair: Jalil Etminan

PELS Chapter Chair: Don Zinger

Computer/Controls Chapter Chair: Rakesh Vasudevan

Stay Connected, Join us on Social Media

Facebook: <https://www.facebook.com/ieeerrvs/>

IEEECollabratec: <https://ieee-collabratec.ieee.org/>

Missed a meeting? Check out our Google Drive for previous presentations.

IEEE RRVS Google Drive: <https://drive.google.com/a/ieee.org/>

1. Login with IEEE account
 2. On the left menu, click "Shared with me".
 3. Click on "Members Folder"
 4. Browse folders for past meeting presentations
-
-



IEEE Personal E-Mail Alias Service

with Free Virus Scanning

The IEEE now offers an **Alias Service** in which all IEEE members can register a **personal alias** of their choice, which will forward E-Mail to their real internet e-mail address. Visit...

Update Your IEEE Member Contact Info Online

<http://www.ieee.org/web/membership/home/index.html>

Join us on Facebook: <https://www.facebook.com/ieerrvs/>
 Join us on LinkedIn: <https://www.linkedin.com/groups/12087034>
 IEEE Collabratec: <https://ieee-collabratec.ieee.org/>

Rock River Valley Section Chapters

Industry Applications Society Chapter
Established 1992

Joint Computer/Control Systems Society Chapter
Established 1995

Power Electronics Society Chapter
Established 1996

Electromagnetic Compatibility Society Chapter
Established 2007

The Rock River Valley Section gratefully acknowledges the following companies and colleges for supporting Section Officers:

[Collins Aerospace](#) • [Northern Illinois University](#) •