Energy Efficient Hardware Security Using Post-CMOS Nanodevices for Mobile Computing

Overview

The security issues in the current-world computer systems are not only limited to software and data threats, but hardware-based security has also become a major concern. Resource-constrained internet of things (IoT) and mobile computing have an intense need for secure hardware systems to address complex security threats. Research suggests that hardware-based security is a key to achieve reliable communication, privacy protection, and data encryption in IoT and mobile computing. Hardware solutions like physically unclonable functions (PUFs), hardware encryption, and true random number generators (TRNGs) have displayed excellent ability to tackle emerging security issues. They show a great promise to identify and resolve security threats such as chip cloning, Trojan insertion, IC recycling, and side-channel attacks. However, conventional CMOS-based hardware security circuits offer limited randomness and entropy along with other drawbacks like high sensitivity to environmental perturbations, area, and power overhead. Emerging logic devices such as symmetric FET, silicon nanowire FET, and non-volatile memories (NVMs) like spin-transfer-torque-magneto resistive RAM (STT-MRAM) and resistive RAM are good candidates to implement hardware security solutions. These devices offer inherent entropy sources to realize hardware security solutions with reduced area and power overhead for mobile computing and IoT.

This course will expose the participants to the basic concept of hardware security primitives and solutions, existing security challenges in IoT, mobile computing and the potential of hardware-based security techniques to overcome these challenges, and new research directions in the field of hardware security solutions, a basic understanding of post-CMOS nanodevices (low power logic and NVMs) for application in a hardware security solution, and the simulation software tools through hands-on experience. Course participants will learn these topics through lectures and hands-on experiments. Also, the case studies will be shared to stimulate the research motivation of participants.

MHRD Scheme on Global Initiative on Academic Network (GIAN)

Course Duration:
December 26, 2022 – December 30, 2022

Course Organized By:
Department of Electronics and Communication Engineering, Indian Institute of Technology Roorkee, Roorkee, Uttarakhand, India.

Course Co-ordinator

Prof. Brajesh Kumar Kaushik
Phone: +91-1332-285662
E-mail: brajesh.kaushik@ece.iitr.ac.in

Course Registration

Course Registration Details	The participation fees for taking the course is as follows: **Participants from abroad : US $250** **Industry/ Research Organizations: INR 5000** **Academic Institutions (Faculty): INR 3000** **Academic Institutions (Students): INR 2000** The above fee includes all instructional materials, computer use for tutorials, laboratory equipment usage charges, 24 hrs free internet facility. The participants will be provided with accommodation on a payment basis. **Number of participants for the course will be limited to 100.**
You Should Attend If…	• you are an executive, engineer, or researcher from manufacturing, service, and government organization including R&D laboratories. • you are a student (BTech/MSc/MTech/PhD) or faculty from a reputed academic and technical institution.

The Faculty

Swaroop Ghosh received the B.E. (Hons.) from IIT, Roorkee and the Ph.D. degree from Purdue University. He is an Associate Professor at Pennsylvania State University. Earlier, he was with the faculty of University of South Florida (USF). Prior to that, he was a Senior Research and Development Engineer in Advanced Design, Intel Corp. His research interests include emerging memory technologies, hardware security, quantum computing and digital testing. Prof. Ghosh served as Associate Editor of the IEEE Transactions On Circuits and Systems I and IEEE Transactions On Computer-Aided Design and as Senior Editorial Board member of IEEE Journal of Emerging Topics on Circuits and Systems (JETCAS). He served as Guest Editor of the IEEE JETCAS and IEEE Transactions On VLSI Systems. He has also served in the technical program committees of more than 25 ACM/IEEE conferences including DAC, ICCAD, CICC, DATE, ISLPED, GLSVLSI, Nanoarch and ISQED. He served as General Chair of ISQED 2021, Conference Chair of ISQED 2020, Program Chair of DAC Ph.D. Forum 2016 and track (co)-Chair of CICC 2017-2019, ISLPED 2017-2021 and ISQED 2016-2017. Prof. Ghosh is a recipient of Intel Technology and Manufacturing Group Excellence Award in 2009, Intel Divisional Award in 2011, Intel Departmental Awards in 2011 and 2012, USF Outstanding Research Achievement Award in 2015, College of Engineering Outstanding Research Achievement Award in 2015, DARPA Young Faculty Award (YFA) in 2015, ACM SIGDA Outstanding New Faculty Award in 2016, YFA Director's Fellowship in 2017, Monkowsky Career Development Award in 2018, Lutron Spira Teaching Excellence Award in 2018, Dean's Certificate of Excellence in 2019 and 2021 and Best Paper Award in American Society of Engineering Education (ASEE) annual conference in 2020. He is a Senior member of the IEEE and the National Academy of Inventors (NAI), Associate member of Sigma Xi and Distinguished Speaker of the Association for Computing Machinery (ACM).

Brajesh Kumar Kaushik received Doctorate of Philosophy (Ph.D.) in 2007 from Indian Institute of Technology, Roorkee, India. He joined Department of Electronics and Communication Engineering, Indian Institute of Technology, Roorkee, as Assistant Professor in December 2009; promoted to Associate Professor in April 2014; and since Aug 2020 he has been serving as full Professor. He had been Visiting Professor at TU-Dortmund, Germany in 2017; McGill University, Canada in 2018, and Liaocheng University, China in 2018. Prof. Kaushik is a Senior Member of IEEE and a member of many expert committees constituted by government and non-government organizations. He is currently serving as Distinguished Lecturer (DL) of IEEE Electron Devices Society (EDS) to offer EDS Chapters with quality lectures in his research domain. He is an Editor of IEEE Transactions on Electron Devices; Associate Editor of IEEE Sensors Journal; Associate Editor of IET Circuits, Devices & Systems; Editor of Microelectronics Journal, Elsevier; Editorial Board member of Journal of Engineering, Design and Technology, Emerald and Circuit World, Emerald. He is among the top 2% scientists in the world as per the Stanford University report of 2019. He is currently serving as a member of two technical committees namely, Spintronics (TC-5), and Quantum Computing, Neuromorphic Computing and Unconventional Computing (TC-16) of IEEE Nanotechnology Council. He is also the Regional coordinator (R10) of IEEE Nanotechnology Council Chapters. He has 12 books to his credit published by reputed publishers such as CRC Press, Springer, Artech, and Elsevier. He has been offered fellowships and awards from DAAD, Shastri Indo Canadian Institute (SICI), ASEM Duo, United States-India Educational Foundation (Fulbright-Nehru Academic and Professional Excellence). His research interests are in the areas of high-speed interconnects, carbon nanotube-based designs, organic electronics, device circuit co-design, optics & photonics-based devices, image processing, spintronics-based devices, circuits and computing.