Authentication and Obfuscation of Integrated Circuits

Prof. Keshab K. Parhi

Dept. of Electrical & Computer Engineering

University of Minnesota, Minneapolis

Email: parhi@umn.edu

<http://ece.umn.edu/~parhi>

Abstract: Physical unclonable functions (PUFs) 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. Examples of memory PUFs include SRAM PUF and DRAM 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. In the second part of the talk, I will talk about 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 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 obfuscation. We will show that the time to find the key by trial and error can be increased exponentially with dynamic obfuscation.

Bio:

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 Distinguished McKnight University Professor and Edgar F. Johnson Professor in the Department of Electrical and Computer Engineering. He has published over 600 papers, is the inventor of 29 patents, and has authored the textbook *VLSI Digital Signal Processing Systems* (Wiley, 1999) and coedited the reference book *Digital Signal Processing for Multimedia Systems* (Marcel Dekker, 1999). His current research addresses VLSI architecture design of signal processing systems, hardware security, data-driven neuroscience and molecular 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, the 2003 IEEE Kiyo Tomiyasu Technical Field Award, the 2001 IEEE W. R. G. Baker prize paper award, and a Golden Jubilee medal from the IEEE Circuits and Systems Society in 2000. He was elected a Fellow of IEEE in 1996 and a Fellow of the AAAS in 2017.