Authentication and Obfuscation of Integrated Circuits

Prof. Keshab K. Parhi
Dept. Electrical & Computer Eng.
University of Minnesota
Minneapolis, MN 55455, USA
Email: Parhi@umn.edu
http://ece.umn.edu/~parhi

Abstract

The problem of hardware security is a serious concern that has led to a lot of work on hardware prevention of piracy and intellectual property (IP), which can be broadly classified into two main categories: 1) authentication-based approach, or 2) obfuscation-based approach. The authentication-based approaches include physical unclonable functions (PUFs) based authentication, digital watermarking, key locking and hardware metering. PUFs can store secret keys in integrated circuits (ICs) by exploiting the uncontrollable randomness due to manufacturing process variations. These PUFs can be used for authentication of devices and for key generation in security applications. Obfuscation-based approach is a technique that transforms an application or a design into one that is functionally equivalent to the original but is significantly more difficult to reverse engineer. Some hardware protection methods are achieved by altering the human readability of the hardware description language (HDL) code, or by encrypting the source code based on cryptographic techniques. Recently, a number of hardware protection schemes have been proposed that modify the finite-state machine (FSM) representations to obfuscate the circuits. This talk will present functional encryption by static and dynamic obfuscation. These obfuscation approaches can prevent reverse engineering and sale of excess parts. .

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 of Electronic Communication in the Department of Electrical and Computer Engineering. He has published over 645 papers, is the inventor of 30 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 machine learning systems, hardware security, data-driven neuroscience and molecular/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, 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 1999. He served as the Editor-in-Chief of *the IEEE Trans. Circuits and Systems, Part-I* during 2004 and 2005. He was elected a Fellow of IEEE in 1996 and a Fellow of the American Association for Advancement of Science (AAAS) in 2017.