Invited Keynote Talk

Trusting The Open Latent IC Backdoors

Farinaz Koushanfar
Electrical and Computer Engineering Department, Rice University
Houston, TX, USA
farinaz@rice.edu

Abstract

Since the Integrated Circuits (ICs) form the core computing and communication kernels for the personal computing, industries, governments and defense in the modern era, ensuring IC trust -- in the presence of untrusted third-party foundries and unidentified supply chains -- has become a major challenge. The prohibitive cost of manufacturing state-of-the-art ICs in nano-meter scales has made the use of contract foundries and third party Intellectual Property (IP) the dominant microelectronics business practice. The hidden backdoors into the chips are a double-edge sword. On one hand, the clandestine backdoors embedded by the reliable designers or trusted supply chain providers enable tracking or having post-fabrication control of the ICs on the production line and while in-use. On the other hand, the latent backdoors (a.k.a., Trojans) implanted by the untrusted third-party manufacturer or unknown supply chain entities enable the potential external adversaries to control, monitor, or to spy the chip software/data contents and communications.

In this talk, we question the contemporary IC backdoor research model directed by interested organizations, primarily defense and government. The talk then suggests better understanding of the hidden backdoor disclosure models to improve the quality and impact of the IC Trust research.

.

Categories & Subject Descriptors: [Hardware]: GENERAL; B.8 [Performance and Reliability]; K.5.1 [Legal Aspect of Computing]: Hardware/Software Protection - Proprietary rights

General Terms: Design, Algorithms, Security.

Bio

Farinaz Koushanfar is an Assistant Professor in the Department of Electrical & Computer Engineering at Rice University, where she is the Director of Texas Instruments (TI) DSP Leadership University Program. Before joining Rice in 2006, she received her Ph.D. in Electrical Engineering and Computer Science and her M.A. in Statistics both from UC Berkeley. Her research focus is in the area of embedded systems. She creates techniques for synthesis and design of embedded systems with an emphasis on customizable, adaptive, lightweight, and secure devices. Her ongoing projects are focused on hardware protection and trust, security of hardware-based and cyber-physical systems, efficient embedded systems design, and emerging technologies and applications. For her contributions, she has received a number of awards and honors including the Presidential Early Career Award for Scientists and Engineers (PECASE) from President Obama, ACM SIGDA Outstanding New Faculty Award, Office of Naval Research (ONR) Young Investigator Program (YIP) Award, Army Research Office (ARO) Young Investigator Program (YIP) Award, National Science Foundation (NSF) CAREER Award, Young Faculty Award from the Defense Advanced Research Projects Agency (DARPA), MIT Technology Review TR-35, Intel Open Collaborative Research (OCR) Fellowship, and a Best Paper Award at Mobicom.

STC'11, October 17, 2011, Chicago, Illinois, USA.
ACM 978-1-4503-1001-7/11/10.