Tutorial T4

All You Need to Know About Hardware Trojans and Counterfeit ICs

Mark (Mohammad Tehranipoor), University of Connecticut
Domenic Forte, University of Connecticut

Abstract

The migration from a vertical to horizontal business model has made it easier to introduce hardware Trojans and counterfeit electronic parts into the electronic component supply chain. Hardware Trojans are malicious modifications made to original IC designs that reduce system integrity (change functionality, leak private data, etc.). Counterfeit parts are often below specification and/or of substandard quality. The existence of Trojans and counterfeit parts creates risks for the life-critical systems and infrastructures that incorporate them including automotive, aerospace, military, and medical systems. In this tutorial, we will cover (i) Background and motivation for hardware Trojan and counterfeit prevention/detection; (ii) Taxonomies related to both topics; (iii) Existing solutions; (iv) Open challenges; (v) New and unified solutions to address these challenges.

Speaker Biographies

Mark (Mohammad Tehranipoor) is currently the F.L. Castleman Associate Professor in Engineering Innovation at the University of Connecticut. His current research projects include: computer-aided design and test for CMOS VLSI designs, reliable systems design at nanoscale, counterfeit electronics detection and prevention, supply chain risk management, and hardware security and trust. Dr. Tehranipoor has published over 200 journal articles and refereed conference papers and has given more than 120 invited talks and keynote addresses since 2006. He has published five books and ten book chapters. He is a recipient of several best paper awards as well as the 2008 IEEE Computer Society (CS) Meritorious Service Award, the 2012 IEEE CS Outstanding Contribution, the 2009 NSF CAREER Award, the 2009 UConn ECE Research Excellence Award, and the 2012 UConn SOE Outstanding Faculty Advisor Award. He serves on the program committee of more than a dozen of leading conferences and workshops. He served as Program Chair of the 2007 IEEE Defect-Based Testing (DBT) workshop, Program Chair of the 2008 IEEE Defect and Data Driven Testing (D3T) workshop, Co-program Chair of the 2008 International Symposium on Defect and Fault Tolerance in VLSI Systems (DFTS), General Chair for D3T-2009 and DFTS-2009, and Vice-general Chair for NATW-2011. He co-founded a new symposium called IEEE International Symposium on Hardware-Oriented Security and Trust (HOST) and served as HOST-2008 and HOST-2009 General Chair and Chair of Steering Committee. He is currently serving as an Associate EIC for IEEE Design & Test, an Associate Editor for JETTA, an Associate Editor for Journal of Low Power Electronics (JOLPE), an IEEE Distinguished Speaker, and an ACM Distinguished Speaker. Dr. Tehranipoor is a Senior Member of the IEEE and Member of ACM and ACM SIGDA. He is currently serving as the director of CHASE center.

Domenic Forte received the B.S. degree in Electrical Engineering from Manhattan College, Riverdale, NY, in 2006 and the M.S. and Ph.D. degrees in Electrical and Computer Engineering from University of Maryland, College Park, MD, in 2010 and 2013 respectively. He is currently an Assistant Professor with the Electrical and Computer Engineering Department, University of Connecticut, Storrs, where he has been since August 2013. His current research interests include anti-counterfeiting for electronic components and devices, trusted and reliable processors
and ICs, and nanoscale integration challenges. Dr. Forte was a recipient of the Northrop Grumman Fellowship and the George Corcoran Memorial Outstanding Teaching Award by the ECE Department, University of Maryland. His work has been recognized through several best paper awards and nominations, including Adaptive Hardware Systems (AHS) 2011 and Design Automation Conference (DAC) 2012.