Contents

1 Background on VLSI Testing  ............................................. 1
   Junxia Ma and Mohammad Tehranipoor

2 Hardware Implementation of Hash Functions  ....................... 27
   Zhijie Shi, Chujiao Ma, Jordan Cote, and Bing Wang

3 RSA: Implementation and Security  ...................................... 51
   Nicholas Tuzzio and Mohammad Tehranipoor

4 Security Based on Physical Unclonability and Disorder .......... 65
   Ulrich Rührmair, Srinivas Devadas, and Farinaz Koushanfar

5 Hardware Metering: A Survey  ............................................. 103
   Farinaz Koushanfar

6 Secure Hardware IPs by Digital Watermark  ............................ 123
   Gang Qu and Lin Yuan

7 Physical Attacks and Tamper Resistance  .............................. 143
   Sergei Skorobogatov

8 Side Channel Attacks and Countermeasures  ......................... 175
   Ken Mai

9 Trusted Design in FPGAs  .................................................. 195
   Mehrdad Majzoobi, Farinaz Koushanfar, and Miodrag Potkonjak

10 Security in Embedded Systems  ......................................... 231
    Yunsi Fei and Juan Carlos Martinez Santos

11 Side-Channel Attacks and Countermeasures
    for Embedded Microcontrollers  ......................................... 263
    Patrick Schaumont and Zhimin Chen
12 Security for RFID Tags .................................................... 283
   Jia Di and Dale R. Thompson

13 Memory Integrity Protection .............................................. 305
   Yin Hu and Berk Sunar

14 Trojan Taxonomy ........................................................... 325
   Ramesh Karri, Jeyavijayan Rajendran, and Kurt Rosenfeld

15 Hardware Trojan Detection ............................................... 339
   Seetharam Narasimhan and Swarup Bhunia

16 Design for Hardware Trust ................................................ 365
   Yier Jin, Eric Love, and Yiorgos Makris

17 Security and Testing ........................................................ 385
   Kurt Rosenfeld and Ramesh Karri

18 Protecting IPs Against Scan-Based Side-Channel Attacks .......... 411
   Mohammad Tehranipoor and Jeremy Lee
Contributors

Swarup Bhunia  Case Western Reserve University, Cleveland, Ohio, USA

Zhimin Chen  ECE Department, Virginia Tech, Blacksburg, VA 24061, USA

Jordan Cote  Computer Science and Engineering Department, University of Connecticut, Storrs, CT, USA

Srinivas Devadas  Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Cambridge, USA

Jia Di  Computer Science and Computer Engineering Department, University of Arkansas, Fayetteville, Arkansas, USA

Yunsi Fei  Department of Electrical and Computer Engineering, University of Connecticut, Storrs, CT, USA

Yin Hu  Worcester Polytechnic Institute, Worcester, MA, USA

Yier Jin  Department of Electrical Engineering, Yale University, New Haven, CT 06520, USA

Ramesh Karri  Polytechnic Institute of New York University, Brooklyn, NY, USA

Farinaz Koushanfar  Electrical and Computer Engineering Department, Rice University, Houston, Texas 77215-1892, USA

Jeremy Lee  DFT Engineer, Texas Instruments, Dallas, TX, USA

Eric Love  Department of Electrical Engineering, Yale University, New Haven, CT 06520, USA

Chujiao Ma  Computer Science and Engineering Department, University of Connecticut, Storrs, CT, USA

Junxia Ma  University of Connecticut, Storrs, CT, USA

Ken Mai  Carnegie Mellon University, 5000 Forbes Avenue, Pittsburgh, PA 15213, USA
Mehrdad Majzoobi  Electrical and Computer Engineering Department, Rice University, 6100 Main, MS380, Houston, TX 77005, USA

Yiorgos Makris  Department of Electrical Engineering, Yale University, New Haven, CT 06520, USA

Juan Carlos Martinez Santos  Department of Electrical and Computer Engineering, University of Connecticut, Storrs, CT, USA
Currently on leave from Universidad Tecnologica de Bolivar, Cartagena, Colombia

Seetharam Narasimhan  Case Western Reserve University, Cleveland, Ohio, USA

Miodrag Potkonjak  Computer Science Department, University of California Los Angeles, Los Angeles, CA 90095-1596, USA

Gang Qu  Electrical and Computer Engineering Department, Institution for Systems Research, University of Maryland, College Park, MD 20742, USA

Jeyavijayan Rajendran  Polytechnic Institute of New York University, Brooklyn, NY, USA

Kurt Rosenfeld  Google Inc., New York, USA

Ulrich Rührmair  Computer Science, Technische Universitat Munchen, Munich, Germany

Patrick Schaumont  ECE Department, Virginia Tech, Blacksburg, VA 24061, USA

Zhijie Shi  Computer Science and Engineering Department, University of Connecticut, Storrs, CT, USA

Sergei Skorobogatov  University of Cambridge, Computer Laboratory, JJ Thomson Avenue, Cambridge CB3 0FD, UK

Berk Sunar  Worcester Polytechnic Institute, Worcester, MA, USA

Mohammad Tehranipoor  UCONN Electrical and Computer Engineering, University of Connecticut, 371 Fairfield Way, Unit 2157 Storrs, CT 06269-2157, USA

Dale R. Thompson  Computer Science and Computer Engineering Department, University of Arkansas, Fayetteville, Arkansas, USA

Nicholas Tuzzio  UCONN Electrical and Computer Engineering, University of Connecticut, 371 Fairfield Way, Unit 2157, Storrs, CT 06269-2157, USA

Bing Wang  Computer Science and Engineering Department, University of Connecticut, Storrs, CT, USA

Lin Yuan  Synopsys Inc., Mountain View, CA 94043, USA