Trustworthy Hardware

By **RAMESH KARRI**
Guest Editor

FARINAZ KOUSHANFAR
Guest Editor

Since the 1990s, there has been a steady trend away from inhouse integrated circuit (IC) design and fabrication toward outsourcing various aspects of design, fabrication, testing, and packaging of ICs. The emergence of such a globalized, horizontal semiconductor business model created hitherto unknown security and trust concerns in the ICs and the information systems (rooted in these ICs), which modern society relies on for mission-critical functionality. IC and system security and trust concerns include threats related to the malicious insertion of Trojan circuits designed to act as silicon time bombs to disable an IC, intellectual property (IP) and IC piracy, untrustworthy third-party IPs, exfiltrating sensitive material from an IC, and malicious system disruption and diversion.

Systems should be made trustworthy and secure hardware up. Security and trust should be considered as a first class metric during all stages in the IC and system design flows side-by-side power, cost, and performance. This special issue showcases advances in state-of-the-art trustworthy ICs and systems, and spans several aspects of IC and system security ranging from theoretical and conceptual foundations, synthesis, testing, and verification, through modeling and optimization, to case studies. From a trustworthy hardware platforms perspective this special issue covers IC and system security and trust issues in application-specific integrated circuits (ASICs), custom off the shelf (COTS), field-programmable gate arrays (FPGAs), microprocessors, and embedded systems. It explains novel hardware security primitives such as physical unclonable functions (PUFs), public PUFs (PPUFs), and random number generators. It presents design for trust techniques such as IC watermarking, fingerprinting, obfuscation, and split manufacturing. It presents hardware-based security protocols for digital rights management (DRM), IC metering, enabling and disabling, and authentication. Finally, it presents a variety of hardware-based attacks.

This special issue showcases advances in state-of-the-art trustworthy integrated circuits and systems spanning a range of topics from theoretical and conceptual foundations, synthesis, and testing to modeling and optimization, and case studies.

The first two papers survey novel hardware-based security primitives. Identification, authentication, and integrity checking are important tasks for ensuring the security and protection of devices, programs, and data. The use of microscopic, random, and unclonable disorder in physical media for such security tasks has recently gained attention. The first paper "Physical unclonable functions and applications: A tutorial" is a tutorial on ongoing work in physical-disorder-based security, security analysis, and implementation choices. The second paper entitled "Public physical unclonable functions" surveys the time-bounded or public PUFs, including their design and security evaluation and the new protocols that they can support.

The following three papers focus on embedded systems security. There is a steady rise of interconnected embedded systems as part of the emerging vision of pervasive computing. The PC-centric Internet is evolving into the Internet of Things. Securing such networked embedded devices is vital. A prominent attack on networked embedded systems is the Stuxnet virus on the nuclear reactor controllers. Another example is the attacks on implanted and wearable

Digital Object Identifier: 10.1109/JPROC.2014.2334837

medical embedded devices. These devices introduce vulnerabilities that may, in the best case, compromise the privacy of a patient and in the worst case may be life threatening. Other examples include hacking critical automotive functions and street light controllers. The paper titled "Microcontrollers as (in)security devices for pervasive computing applications" discusses threats to microcontroller-based embedded systems, using two detailed case studies. The paper titled "Trustworthiness of medical devices and body area networks" surveys the threat landscape of medical embedded devices and the merits and shortcomings of existing defenses. The next paper in embedded security titled "Mobile trusted computing" surveys the trusted computing features in historical computing systems as well as in state-of-the-art mobile computing systems by focusing on features such as hardware support for platform integrity, attestation, secure storage, isolated execution, authentication, and provisioning.

The next two papers are on attacks on ICs. Counterfeiting of ICs has been on the rise, impacting the security and reliability of electronic systems. Reports show that recovered ICs are a significant percent of all counterfeit ICs in the market. Such ICs are recovered from scrapped boards of used devices. Identification of such counterfeit ICs is a challenge since these ICs are identical in appearance and functionality and package to fresh ICs. The paper titled "Counterfeit integrated circuits: A rising threat in the global semiconductor supply chain" surveys the state of the art in counterfeiting and detection technologies. Another attack on ICs entails insertion, deletion, or malicious modifications in ICs. This attack can be launched at multiple points in the supply chain, ranging from the third-party IP cores to the foundry that fabricates the ICs. The paper "Hardware Trojan attacks: Threat analysis and countermeasures" provides a comprehensive survey of the state-of-the-art Trojan attacks, modeling, and countermeasures.

Using FPGAs, a designer can separate the design process from the manufacturing flow. Sensitive designs need not be exposed to possible theft and tampering during their manufacture. However, there are other vulnerabilities introduced by FPGAs, such as the ability of an attacker to change the design by modifying or replacing the FPGA programming bit stream. The paper titled "FPGA security: Motivation, features, and applications" discusses all aspects of FPGA security and trust.

While hardware security and trust is a relatively recent concern, a somewhat similar yet fundamentally different problem of manufacturing defects has been extensively explored in the adjacent domain of very large scale integration (VLSI) test. Whereas the IC level attacks are man made, intentional, and hidden, manufacturing defects are unintentional. The paper titled "Regaining trust in VLSI Design: Design-for-trust techniques" surveys how concepts in VLSI test, such as fault analysis and delay tests, can be adopted in the context of hardware security and trust. Inspired by the design-for-testability (DfT) for better testability of manufacturing defects, this paper reviews design-for-trust (DfTr) solutions.

The final paper in this special issue, "A primer on hardware security: Models, methods, and metrics," presents a novel primer on hardware security threat models, metrics, and remedies. The existing literature in this domain, however rich, assumes *ad hoc* models, solutions, and metrics, which lead to difficulty in analysis and comparison of the methodologies. This paper discusses the first of this kind classification of the underlying threat models, state-of-the-art defenses, and evaluation metrics for the following important hardware-based vulnerabilities: hardware malware (Trojan), reverse engineering, side channels, counterfeiting, overbuilding, and/or piracy of the pertinent IPs. The classifications provide a guide for the academics and practitioners to clearly state the assumptions and problems, while fairly evaluating their solutions and building stronger countermeasures. The new systematization of knowledge that is provided by this work will pave the way for a more rapid and organized progress in this field.

In a nutshell, the increasing number of security threats and the cost of compromised systems are elevating security to be a first-order design requirement in computer systems side by side the requirements of speed, power, cost, and programmability. Consequently, similar to the design for manufacturability and design for testability mantras of the past, design for trust should be the new mantra to combat this very important threat. ■

Acknowledgment

The guest editors would like to thank the contributors to this special issue and the reviewers—thought leaders and domain experts in hardware security—for making the guest editors' task much easier and enjoyable notwithstanding the tight timeline. Special thanks go to Dr. C. Wang, Division Director in the U.S. Army Research Office (ARO), for helping organize a workshop on trustworthy hardware in New York City in fall 2013; several of the papers were derivatives of the presentations at this workshop. The guest editors would also like to thank the Managing Editor Vaishali Damle and the Publications Editor of the Proceedings of the IEEE Jo Sun for helping manage this special issue. The work of the guest editors was supported in part by NYU/NYU-AD Center for Research in Information Security Studies and Privacy (CRISSP); the National Science Foundation (NSF) under Grants 1319841, 1059328, and 0966187; and ARO.

ABOUT THE GUEST EDITORS

Ramesh Karri received the Ph.D. degree in computer science from the University of California at San Diego, La Jolla, CA, USA.

He is a Professor of Electrical and Computer Engineering at the Polytechnic School of Engineering, New York University, Brooklyn, NY, USA. His research interests include trustworthy integrated circuits (ICs) and processors, high assurance nanoscale IC architectures and systems, very large scale integration (VLSI) design and test, and interaction between security and reliability. He has over 150 journal and conference publications in these areas. He is the Area Director for Cyber Security of the NY State Center for Advanced Telecommunications Technologies at NYU-Poly, Hardware Security Lead of the Center for Research in Interdisciplinary Studies in Security and Privacy (CRISSP, http://crissp.poly.edu/), cofounder of the Trust-Hub (http://trust-hub.1102 org/), and organizer of the annual red team blue team event at NYU, the Embedded Systems Security Challenge (http://esc.isis.poly.edu).

Prof. Karri was the recipient of the Humboldt Fellowship and the National Science Foundation CAREER Award, and Best Student Paper Awards at the 2013 ACM Conference on Computer and Communications Security, the 2013 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems, and the 2011 IEEE VLSI Design Conference. He cofounded and served as the Chair of the IEEE Computer Society Technical Committee on Nanoscale Architectures. He is a cofounder and steering committee member of the IEEE/ACM Symposium on Nanoscale Architectures (NANOARCH), Program Chair (2012) and General Chair (2013) of the IEEE Symposium on Hardware Oriented Security and Trust (HOST), Program Co-Chair (2012) and General Co-Chair (2013) of the IEEE Symposium on Defect and Fault Tolerant VLSI and Nanotechnology Systems, and the General Chair of the 2013 NANOARCH. He serves on several program committees, including VTS, DAC, HOST, and ICCD. He is the Associate Editor of the IEEE Transactions on Information Forensics and Security, the IEEE Transactions on Computer-Aided Design, and the *ACM Journal of Emerging Technologies in Computing*. He is an IEEE Computer Society Distinguished Visitor and has organized invited tutorials on trustworthy hardware (including at the 2012 VLSI Test Symposium, the 2012 International Conference on Computer Design, the 2013 IEEE North Atlantic Test Workshop, the 2013 Design Automation and Test in Europe, the 2013 International Test Conference, and the 2014 IEEE/ACM Design Automation Conference).

Farinaz Koushanfar received the B.S. degree in electrical engineering from Sharif University of Technology, Tehran, Iran, in 1998, the M.S. degree from the University of California Los Angeles (UCLA), Los Angeles, CA, USA, and the M.A. degree in statistics and the Ph.D. degree in electrical engineering from the University of California Berkeley, Berkeley, CA, USA, in 2005.

She is an Associate Professor of Electrical and Computer Engineering (ECE) at Rice University, Houston, TX, USA. She is the Director of the Adaptive Computing and Embedded Systems (ACES) Laboratory.