Guest Editors' Introduction: Confronting the Hardware Trustworthiness Problem

Mohammad Tehranipoor
University of Connecticut

Farinaz Koushanfar
Rice University

THE EMERGENCE OF a globalized, horizontal semiconductor business model raises concerns involving the security and trust of the information systems on which modern society is increasingly reliant for mission-critical functionality. Hardware security and trust issues span a broad spectrum of topics ranging from the malicious insertion of Trojan circuits designed to act as a silicon time bomb to disable a chip upon activation, to intellectual property (IP) and IC piracy, to digital rights management, to untrusted third-party IP cores, to attacks designed to extract encryption keys and IP from a chip, and to malicious system disruption and diversion.

Traditionally, hardware-based security techniques and countermeasures modify hardware to prevent attacks and to protect IP or secret keys. Some of the emerging types of attacks covered by this special issue are fundamentally different. The attacker is assumed to maliciously alter the design before or during fabrication. Trojans can be inserted into a circuit or system developed by a third-party IP vendor, system integrator, or foundry. Detection of such alterations (i.e., hardware Trojans) is extremely difficult since

- a very large number of IP cores, developed by third-party IP vendors located across the world, are used in today's SoCs (verifying the trustworthiness of each IP is an extremely challenging task since there is no golden IP to compare against);
- Trojan circuits are by design activated under rare conditions, which makes them difficult to activate and detect using random/functional/structural stimuli; and
- the adversary can design or configure the Trojan to have a minimal impact on the chip's parametric information, thus the Trojan may not be easily detected using side-channel signal analysis methods.

Accordingly, this special issue covers some of the emerging security and trust issues in various types of electronic devices and systems. The topics of interest for this special issue were Trojan detection and isolation, authenticating the foundry of origin, watermarking, IC metering, physical unclonable functions (PUFs), hardware intrusion detection and prevention, scan-chain encryption, and IP trust. We received a good number of articles covering these areas.

Five papers were selected for publication. The first article in this special issue, "A Survey of Hardware Trojan Taxonomy and Detection" by Mohammad Tehranipoor and Farinaz Koshanfar, discusses the vulnerabilities in today's design and fabrication processes as well as possibility of malicious circuit insertion into a design that can impact the design's functionality or enable transmitting key information to the adversary. The hardware Trojan detection problem has gained significant attention over the past few years, and in this article the authors have provided a detailed overview and analysis of the current state of knowledge in this area.

The second article, "Hardware Trojans in Wireless Cryptographic ICs" by Yier Jin and Yiorgos Makris, studies the problem of hardware Trojans in wireless cryptographic ICs. Using a mixed-signal SoC, the authors demonstrate that simple malicious modifications to the digital part of a wireless cryptographic chip would suffice to leak information without changing the more sensitive analog part. The authors designed two hardware Trojans, which leak the encryption key by manipulating the transmission amplitude or frequency. The Trojans have been designed in such

0740-7475/10/$26.00 © 2010 IEEE Copublished by the IEEE CS and the IEEE CASS

a way that they change neither the functionality of the digital part nor the performance of the analog part, and their impact on the wireless transmission parameters can be hidden within the fabrication process variations. The authors present an advanced statistical analysis for the transmission power to reveal a Trojan's presence.

The third article, "Attacks and Defenses for JTAG" by Kurt Rosenfeld and Ramesh Karri, addresses some security issues surrounding JTAG. The authors investigate the threat of a malicious chip in a JTAG chain. They outline attack scenarios where trust in a digital system is downgraded by the presence of such a chip in the system. To defend against this, the authors propose a protection scheme that hardens JTAG by making use of lightweight cryptographic primitives, namely stream ciphers and incremental message authentication codes. The scheme defines four levels of protection. For each of the attack scenarios, the authors determine which protection level is needed to prevent it.

The fourth article, "Secure and Robust Error Correction for Physical Unclonable Functions" by Meng-Day (Mandel) Yu and Srinivas Devadas, proposes a new and secure error correction method for PUFs. Error correction is commonly used to stabilize the PUF responses in the presence of environmental and operational conditions. Conventional error correction methods leak information that could compromise the PUF security. To limit the information leakage, a new coding method, called *index-based syndrome* coding, is devised. IBS is shown to be information theoretically secure. The security and reliability of the method are also affirmed by the NIST randomness tests, and by proof-of-concept implementation on a Xilinx Virtex-5 FPGA.

Finally, the last article, "Preventing IC Piracy Using Reconfigurable Logic Barriers" by Alex Baumgarten, Akhilesh Tyagi, and Joseph Zambreno, addresses IC piracy prevention. The approach adds reconfigurable logic barriers to the IC pre-fabrication. These barriers separate the inputs from the outputs such that every path from inputs to outputs passes through a barrier. The IC would function correctly only when the correct keys are applied to the barriers. The barrier insertion heuristic utilizes the don't-care sets and the node locations in the network to maximize the reverse-engineering effort while limiting the overhead.

We sincerely hope that you will enjoy reading this special issue, and we would like to thank all authors and reviewers for their tremendous efforts and contribution in producing these high-quality articles. We also take this opportunity to thank the previous Editor in Chief (EIC) Tim Cheng and current EIC Krishnendu Chakrabarty, and the entire *Design & Test* editorial staff for their encouragement and assistance in producing this special issue. ■

Mohammad Tehranipoor is an assistant professor of electrical and computer engineering at the University of Connecticut, Storrs. His research interests include CAD and test for CMOS VLSI designs and emerging nanoscale devices, DFT, at-speed test, secure design, and IC trust. He has a PhD in electrical engineering from the University of Texas at Dallas. He is a senior member of the IEEE and a member of the ACM and ACM SIGDA.

Farinaz Koushanfar is an assistant professor of electrical and computer engineering and the director of Texas Instruments DSP Leadership at Rice University. Her research interests include hardware trust and IP protection, computer and communication system security, design and analysis of adaptive systems, and emerging technologies. She has a PhD in electrical engineering and computer science from the University of California, Berkeley. She is a senior member of the IEEE and a member of the ACM and the American Association for the Advancement of Science.

■ Direct questions and comments about this article to Mohammad Tehranipoor, Electrical and Computer Engineering Dept., University of Connecticut, 371 Fairfield Way, Unit 2157, Storrs, CT 06269-2157; tehrani@engr.uconn.edu.