Guest Editors’ Introduction: Trusted System-on-Chip with Untrusted Components

Swarup Bhunia  
Case Western Reserve University

Dakshi Agrawal  
IBM TJ Watson Research Center

Leyla Nazhandali  
Virginia Tech

**Security of electronic hardware at different stages of its life cycle has emerged as a paramount concern to integrated circuits (ICs) designers, system integrators, as well as to the end users. Over time, hardware components, platforms and supply chains have been considered secure and trustworthy. However, recent discoveries and reports on security vulnerabilities with attacks in microchips and circuits violate this hardware root of trust. System-on-Chip (SoC) design based on reusable hardware intellectual property (IP) is now a pervasive design practice in the industry due to the dramatic reduction in design/verification cost and time to market offers. This growing reliance on reusable pre-verified hardware IPs and a wide array of design automation tools during SoC design—often gathered from untrusted third party vendors—severely affects the security and trustworthiness of SoC computing platforms. Major security issues at different stages of SoC life cycle include piracy during IP evaluation, reverse engineering, cloning, counterfeiting, as well as malicious hardware modifications, commonly referred to as hardware Trojan attacks. Furthermore, use of untrusted foundries in a fabless business model greatly aggravates the SoC security threats. Because of evergrowing computing demands, modern SoCs tend to include many heterogeneous processing cores (e.g., MPSoC), scalable communication network, and reconfigurable fabric (for instance, embedded FPGA), in order to incorporate logic that will likely change, as standards and requirements evolve. Such design practices greatly increase the number of untrusted components in an SoC design and make the overall system security a pressing concern.

Clearly, there is a critical need to develop low-cost effective countermeasures that are based on the rigorous analysis of SoC security issues. It is important to consider various attack models that arise out of the involvement of multiple untrusted entities such as IP vendors, design tool developers, and foundries in the design cycle. These countermeasures should enable trusted operation with untrusted components at acceptable hardware overhead and design/validation cost. Towards that end, this special issue presents six articles that highlight challenges and approaches related to improving security and trustworthiness of SoC. The articles cover a wide range of security issues and innovative solutions related to IP-based SoC design, manufacturing, and test process.

The first article titled “Practical, Lightweight Secure Inclusion of Third-Party Intellectual Property” by Waksman et al., proposes a secure, practical, and lightweight process for using third-party reusable intellectual property (IP). A decision-making algorithm called Algorithm for Resisting Trojans (ART) has been proposed that combines several existing techniques into one. The effectiveness
of the algorithm has been demonstrated through implementation of a microcontroller in which all design modules are secured against digital design-level Trojans.

This is followed by an article by Aarestad et al., titled “HELP: A Hardware-Embedded Delay PUF” that proposes a new Physical Unclonable Function (PUF) and uses the natural variations in the path delays of a core macro on a chip to generate unique PUF responses. The core macro used in this work is Advanced Encryption Standard (AES). The challenges to HELP are inputs to the AES core and the responses are derived from digitized path delays of the outputs. Output bit strings are generated by comparing pairs of path delays. The effectiveness of the HELP has been demonstrated with its functional implementation on 29 Xilinx VirtexPro(V2Pro) FPGA boards.

The next article titled “A Clock Sweeping Technique for Detecting Hardware Trojans Impacting Circuits Delay” by Xiao et al., shows how a clock control technique can be used to obtain the critical and noncritical path delay, and how these delays can be used to generate signatures for the purpose of detecting hardware Trojans. With the help of simulations and FPGA results, the authors demonstrate the effectiveness of their method under process variations, even for Trojans as small as a few gates.

This is followed by an article by Rajendran et al., titled “Securing Processors Against Insider Attacks: A Circuit-Microarchitecture Co-Design Approach” that analyzes the issue of insider attack in the case of a microprocessor, and presents an effective countermeasure using a circuit-architecture codesign approach. It presents a new circuit-hardening approach based on logic encryption to protect against malicious hardware modifications or Trojan attack. The hardening step either makes a Trojan nonfunctional or improves the detection sensitivity for efficient Trojan identification with exiting approaches. The authors experimentally demonstrated the efficacy of the method for the OpenSPARC T1 microprocessor and presented performance and area overhead.

The next article titled “Hardware Trojan Insertion by Direct Modification of FPGA Configuration Bitstream” by Chakraborty et al., demonstrates the feasibility of purely software-enabled malicious modification to insert hardware Trojan in circuits mapped to FPGA—all based on public domain information. The article suggests some possible risk mitigation approaches in the context of the demonstrated attack.

The final article titled “Eliminating Timing Information Flows in a Mix-Trusted System-on-Chip” by Oberg et al., addresses the issue of acquisition and integration of untrusted third-party IP cores during SoC design process. In order to establish trusted SoC design, it presents an approach to ensure information flow isolation between a trusted and an untrusted component. The paper proposes the use of gate-level information flow monitoring to track the security level of every bit of information. Effectiveness of the approach is demonstrated with an example for SoC design.

These articles provide a glimpse to the various issues and technologies that are likely to shape the world of secure and trusted SoC design and their in-field operation. We hope that they introduce new concepts, tickle your intellect, and spur innovation in this field of growing importance.

Acknowledgment

This special issue resulted from the inputs and efforts of many individuals to whom we are thankful. We received several high-quality articles, which were further strengthened through detailed comments and suggestions from a host of reviewers. We are grateful for their time and commitment. Further, we appreciate the insightful “Last Byte” by Prof. Srin Devadas that provides an apt ending to the issue. We thank the former IEEE Design and Test Editor-in-Chief Krishnendu Chakrabarty and current Editor-in-Chief André Ivanov for their continued support throughout this process. And finally, the editorial staff of the IEEE Publishing Operations deserve special thanks for their wonderful job in editing and organizing this issue.

Swarup Bhunia is an associate professor of Electrical Engineering and Computer Science at Case Western Reserve University, Cleveland, OH, USA. He received his MTech from the Indian Institute of Technology (IIT), Kharagpur, and his PhD in electrical engineering from Purdue University, West Lafayette, IN, USA, in 1997 and 2005, respectively. Prof. Bhunia has over ten years of research and development experience with over 150 publications.
in peer-reviewed journals and premier conferences in the area of hardware security and energy-efficient electronics. He has worked in the semiconductor industry on RTL synthesis, verification, and low-power design for about three years.

**Dakshi Agrawal** is a Research Staff Member, Manager at IBM Thomas J. Watson Research Center, Yorktown Heights, NY, USA. He received his BTech in 1993 from the Indian Institute of Technology-Kanpur (IITK), his MS in 1995 from the Washington University, St. Louis, MO, USA, and his PhD in 1999 from the University of Illinois-Urbana-Champaign (UIUC), Urbana, IL, USA, all in electrical engineering. Dr. Agrawal has worked in the areas of Networking and Security since 1999 at IBM Research. He is an IBM Master Inventor with more than 50 granted or filed patents. For his technical contributions, he has been recognized by several high-prestige internal awards by IBM and is a Fellow of the IEEE.

**Leyla Nazhandali** is an associate professor in the Bradley Department of Electrical and Computer Engineering at Virginia Tech. She received her BS degree in electrical engineering from Sharif University of Technology, Iran, in 2000. She then pursued her graduate studies in computer engineering at the University of Michigan, receiving her MS and PhD degrees in 2002 and 2006, respectively. Her research interests are in energy-constrained circuits and architecture, and secure embedded hardware design. Dr. Nazhandali is the recipient of the prestigious National Science Foundation CAREER award in 2008 and the winner of IEEE Real World Engineering Projects Contest.

Direct questions and comments about this article to Swarup Bhunia, Electrical Engineering and Computer Science, Case Western Reserve University, 10900 Euclid Avenue, Glennan Bldg, Cleveland, OH 44106 USA; skb21@case.edu.