Guest Editorial

Hardware-Assisted Techniques for Security and Protection in Consumer Electronics

I. Introduction

We present a special issue on "*Hardware - Assisted Techniques for Security and Protection in Consumer Electronics*" in IET Computers and Digital techniques. This special issue encompasses novel solutions for any security/protection problems related to hardware used in CE. Consumer electronics (CE) comprises high end devices ranging from digital camera, multi-spectral camera, IP TV, smart tablets, night vision camera to smart meter, along with the information and communication technology that make emerging smart cities and Internet of Things (IoT) a reality. In the world of CE and IoT, security, privacy, and protection of hardware and its information are equally important. We define "Hardware-Assisted Security" as the security/protection of hardware/IP core of CE devices or information by a hardware/system of CE devices. The term "security" encapsulates a broad theme that covers many aspects including hardware security, protection, privacy, trustworthiness, and intellectual property (IP) protection and information security. System security may refer to the security of the system (e.g. a specific CE device) that handles the data or information. In a CE based framework, security and protection of its hardware and intellectual property (IP) cores are considered major challenges. Thus, the use of secured IPs is of paramount importance. In the era of smart cities, swelling CE hardware design complexity is out-striding designer productivity, ensuing into greater endeavours. Further, the current approach to CE device and system design is massively dependent on global IP supply chains. To maximize design productivity and minimize design time the use of IP cores, often delivered by a third party vendor, has become a de-facto practice in the industry. It is also estimated that counterfeits could have an increasingly significant impact on the semiconductor market. However, rising threats to security and surging piracy issues threaten global supply chains as CE system-on-chip (SoC) design becomes increasingly commoditised.

II. Topics of Special Issue

This special issue is comprised of six articles. These 6 articles were selected after a rigorous review which was under taken by the guest editors with the help of reviewers spanning over several months. The 6 articles cover NBTI stress attack detection, Trojan detection, and hardware based solutions for security. We briefly present the articles in the rest of this Section.

(1) Paper entitled "*Circuit Enclaves Susceptible to Hardware Trojans Insertion at Gate-Level Designs*" by Seyyed Mohammad Sebt, Ahmad Patooghy, Hakem Beitollahi, Michel Kinsy introduces efficient net susceptibility metrics to significantly speedup functional-HT detection in gate-level digital designs. The proposed metrics perform a computationally low overhead analysis on the controllability and observability parameters of each net of the under HT-test circuit.

(2) Paper entitled "*Signal Word-Level Statistical Properties-based Activation Approach for Hardware Trojan Detection in DSP Circuits*" by Qiang Liu, He Li. The paper introduces a novel approach for efficiently activating Trojans hidden in DSP circuits by increasing the transition activity of rare bits. the proposed approach can generate appropriate test vectors, which effectively activate internal rare nodes and trigger Hardware Trojans (HTs).

(3) Paper entitled "*Effect of NBTI Stress on DSP cores used in CE Devices: Threat Model and Performance Estimation*" by Anirban Sengupta, Deepak Kachave, Shubha Neema, Sri Harsha P presents a novel reliability and threat analysis of negative bias temperature instability (NBTI) stress on digital signal processing (DSP) cores.

(4) Paper entitled "*A New, Low-Complexity and DPA-Resistant Two-folded Power-Aware RSA Security Schema Implementation for IoT-Connected devices*" by Mohammad Ali Doostari, Saman Kaedi, M. B. Ghaznavi-Ghoushchi proposes new implementation schema for hierarchically-connected Internet-of-Things-Devices for indoor applications. This schema allows the IoT network to utilize strong-crypto-algorithms (i.e. RSA) instead of lightweight-algorithms (i.e. ABE).

(5) Paper entitled "*P2M-Sec: Security Enhancement using Combined PUF and PRNG Model for Authenticating Consumer Electronic Devices*" by Paul Wortman, Fatemeh Tehranipoor, Wei Yan, John Chandy presents a novel method of using various physically unclonable functions (PUFs) as a potential seed for a pseudo random number generators (PRNGs) element. These can be used to authenticate consumer electronic devices or protect communication over a large interconnected network.

(6) Paper entitled "*A Practical Realization of a Return Map Immune Lorenz Based Chaotic Stream Cipher in Circuitry*" by Ava Hedayatipour, Daniel Brown, Md Majumder, Garrett Rose, Nicole McFarlane, Donatello Materassi introduces time-scaling factor to obfuscate modulation process of single system parameter to transmit it securely through the single shared state. The paper proposes realization of this process in real-time analog circuitry using on-the-shelf components and minimal processing power.

III. Conclusions

All of the papers selected for this Special Issue show that "Hardware - Assisted Techniques for Security and Protection in Consumer Electronics" is a very important topic of research and investigation of research community. There are several developments happening in this field which this special issue tried to cover and present in a comprehensive manner. We are pleased with the technical depth and spectrum of this special issue, though we readily confess that many aspects of the security problems are not addressed by this special issue. We sincerely thank all the authors and reviewers for their timely efforts, and the Editor-in-Chief and Staff Members for their guidance.

Anirban Sengupta
Indian Institute of Technology (IIT) Indore, India
Email: asengupt@iiti.ac.in

Saraju P. Mohanty
University of North Texas, Denton USA
Email: Saraju.Mohanty@unt.edu

Garrett S. Rose
University of Tennessee, USA
Email: garose@utk.edu

IV. About the Guest Editors

Anirban Sengupta is a Tenured Faculty in the Discipline of Computer Science and Engineering at Indian Institute of Technology (IIT) Indore. He is an IEEE Senior Member. He has authored more than 170 peer-reviewed publications and patents. More than a dozen of his IEEE publications have appeared in 'Top 50 Most Popular Articles' from IEEE Periodicals. His patents have been cited in various industry patents of IBM Corporation, Siemens Corporation, Qualcomm, Amazon Technologies, Siemens Aktiengesellschaft (Germany), Mathworks Inc etc multiple times. His is recipient of several awards/honors such as IEEE Distinguished Lecturer by the Consumer Electronics Society in 2017, IEEE Computer Society TCVLSI Outstanding Editor Award in 2017 and IEEE Computer Society TCVLSI Best Paper Award in IEEE iNIS 2017. He holds around 12 Editorial positions in various Transactions and Journals. He is the Editor-in-Chief of IEEE VCAL (IEEE Computer Society TCVLSI), and General Chair of 37th IEEE International Conference on Consumer Electronics (ICCE) 2019, Las Vegas. More information is available at: www.anirban-sengupta.com

Saraju P. Mohanty is a Professor at the University of North Texas. Prof. Mohanty's research is in "Smart Electronic Systems" which has been funded by National Science Foundations, Semiconductor Research Corporation, US Air Force, and Indo-US Science and Technology Forum. He has authored 280 research articles, 3 books, and invented 4 US patents. His Google Scholar h-index is 29 and i10-index is 90. He has received 4 best paper awards and has delivered multiple keynote talks at various International Conferences. He received IEEE-CS-TCVLSI Distinguished Leadership Award in 2018 for services to the IEEE, and to the VLSI research

community. He has been recognized as a IEEE Distinguished Lecturer by the Consumer Electronics Society (CESoc) since 2017. He was conferred the Glorious India Award in 2017 for his exemplary contributions to the discipline. He received Society for Technical Communication (STC) 2017 Award of Merit for his outstanding contributions to IEEE Consumer Electronics Magazine. He was the recipient of 2016 PROSE Award for best Textbook in Physical Sciences & Mathematics from the Association of American Publishers for his Mixed-Signal System Design book published by McGraw-Hill in 2015. He was conferred 2016-17 UNT Toulouse Scholars Award for sustained excellent scholarship and teaching achievements. He is the Editor-in-Chief (EiC) of the IEEE Consumer Electronics Magazine (CEM). He serves as the Chair of Technical Committee on VLSI, IEEE Computer Society.

Garrett S. Rose has been an Associate Professor in the Department of Electrical Engineering and Computer Science at the University of Tennessee since 2014. He received the B.S. in Computer Engineering from Virginia Tech in 2001. He received the M.S. and Ph.D. degrees in Electrical Engineering from the University of Virginia in 2003 and 2006, respectively. From 2006 through 2011 he was an Assistant Professor with the Electrical and Computer Engineering Department at Polytechnic University (now NYU Tandon School of Engineering) in Brooklyn, NY. From 2011 through July 2014 he was a Senior Electronics Engineer with the Air Force Research Laboratory, Information Directorate in Rome, NY. Through his career, his research interests have been focused in the area of nanoelectronic circuit design as applied to a range of applications, including reconfigurable computing, neuromorphic computing and hardware security. More information is available on his website: http://web.eecs.utk.edu/~grose4/