Guest Editorial Special Section on Security Challenges and Solutions With Emerging Computing Technologies

MULTIPLE emerging computing technologies based on, e.g., graphene, spintronics, resistive RAM, quantum computing, and others are being developed to enhance the capabilities of logic devices and circuits. The rapid growth in these technologies is synchronized with the decline of Moore's law, thus promises to herald the era of Beyond CMOS technologies with a significant improvement in energy efficiency, reliability, performance, and manufacturability. These devices enable very different computing paradigms, e.g., neuromorphic computing, non-Boolean computing, and in-memory computing, thus making these platforms an interesting playground for circuit and application-developers alike.

In this special section, we have put together the application of these new technologies in novel circuits and secure system designs.

For example, a number of emerging devices have exhibited interesting security-specific properties to assure security and privacy of computation as an added functionality. The security features of emerging devices support the recent consensus on inclusion of security as a design figure of merit along with conventional metrics, such as power, area, performance, and resilience. However, several of these devices have also opened up new information side channels that require careful analysis before using those as implementation platforms for cryptographic primitives. On one hand, phenomenon such as crosstalk in these devices can threaten well-founded countermeasures, such as masking, which assume independence of the mask values. Likewise, fault tolerance of these devices in the context of security needs a fresh evaluation. On the other hand, for many practical use cases, such as IoT/CPS, and emerging cryptographic standards, such as postquantum cryptography, the security kernels and countermeasures need to be designed with stringent constraints on area/energy footprints. Therefore, identifying suitable design choices and adapting them to different applications in the IoT/CPS context are the need of the hour. In essence, both the design and attack paradigms for secure systems are blended with the emergence of new computing technologies, which are covered in this special section.

The articles were solicited for this special section through a widely circulated call. Out of 18 submissions in total, six were accepted for the final publication. Each article underwent a rigorous review process with multiple iterations. The first three articles focus on the design of security primitives using emerging devices, while the remaining three articles examine various threat vectors and developed countermeasures. A brief highlight of the articles is provided in the following for curious readers.

The first article, "An asynchronous and low-power true random number generator using STT-MTJ" by Perach and Kvatinsky, leverages the entropy existing in the stochastic switching time of the magnetic tunnel junctions (MTJs). This resulted in a true random number generator (TRNG) that not only exhibits excellent randomness but also achieves low power by decoupling from the system clock. The design is evaluated using numerical simulations, including process variations.

The second article, "Low-complexity compressed-sensing-based watermark cryptosystem and circuits implementation for wireless sensor networks" by Chen *et al.*, presents an interesting combination of compressive sensing and its susceptibility to measurement noise to derive a lightweight watermark for sensor nodes. Using this watermark, a protocol is proposed to thwart multiple attacks, including Denial of Service (DoS). The design is implemented and fabricated using 40-nm CMOS technology.

The third article, "Design and evaluation of a printed analog-based differential physical unclonable function" by Zimmermann *et al.*, talks about physical unclonable function (PUF). PUFs are being adopted widely as a technique to establish the identity for a circuit. In this article, printed electronic circuits are used to design a PUF. The design has actually been fabricated, demonstrating excellent properties.

PUFs are also susceptible to cloning attacks. The fourth article, "A spintronics memory PUF for resilience against cloning counterfeit" by Ben Dodo *et al.*, investigates a PUF design based on STT-MRAM. It shows that back-side tampering of the circuit can lead to highly exploitable weaknesses of the design. Subsequently, a tamper-resilient design has been proposed.

The fifth article, "Reversible circuits: IC/IP piracy attacks and countermeasures" by Saeed *et al.*, looks into the futuristic technologies that rely on reversible circuits/devices. These circuits could be subjected to IP piracy and, consequently,

Digital Object Identifier 10.1109/TVLSI.2019.2945850

Trojan insertions. This article proposes modifications of the synthesis flow that makes it much harder for an attacker to reverse engineer the process.

The sixth article, "Design for test and hardware security utilizing retention loss of memristors" by Gong *et al.*, investigates the attacks exploiting scan chain structures of modern ICs. To prevent such attacks, a scan chain design based on memristors is proposed. A secure scan design is obtained by utilizing the retention loss of the memristor devices.

We would like to thank the authors for submitting articles for this special issue. We also express our sincere gratitude to the reviewers for providing high-quality reviews to enhance the quality of the accepted articles. We are indebted to Dr. Massimo Alioto, Editor-in-Chief of the IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS, for his consistent support throughout the review and selection process. We hope that the readers will find this special section stimulating and that it will foster the development of cross-disciplinary themes encompassing security and compute models using emerging computing technologies.

ANUPAM CHATTOPADHYAY, *Guest Editor*
School of Computer Science and
Engineering
Nanyang Technological University
Singapore 639798

SWAROOP GHOSH, *Guest Editor*
School of Electrical Engineering
and Computer Science
Pennsylvania State University
State College, PA 16802 USA

WAYNE BURLESON, *Guest Editor*
Electrical and Computer Engineering
Department
University of Massachusetts Amherst
Amherst, MA 01003-9284 USA

DEBDEEP MUKHOPADHYAY, *Guest Editor*
Department of Computer Science
and Engineering
IIT Kharagpur
Kharagpur 721302, India

Anupam Chattopadhyay (SM'14) received the B.E. degree from Jadavpur University, Kolkata, India, in 2000, the M.Sc. degree from ALaRI, Lugano, Switzerland, in 2002, and the Ph.D. degree from RWTH Aachen University, Aachen, Germany, in 2008.

From 2008 to 2009, he was a Member of Consulting Staff with CoWare R&D, Noida, India. From 2010 to 2014, he led the MPSoC Architectures Research Group, RWTH Aachen, as a Junior Professor. Since September 2014, he has been an Assistant Professor with the School of Computer Science and Engineering, Nanyang Technological University, Singapore, where he was promoted to Associate Professor with tenure in August 2019. He held visiting positions at the Politecnico di Torino, Turin, Italy; EPFL, Lausanne, Switzerland; Technion, Haifa, Israel; and the Indian Statistical Institute, Kolkata. He currently leads multiple projects in the areas of computer architectures, security, design automation, and emerging technologies. His research advances have been reported in more than 100 conference/journal articles (ACM/IEEE/Springer), multiple research monographs and edited books (CRC and Springer), and open-access forums. Together with his doctoral students, he proposed novel research directions, such as domain-specific high-level synthesis for cryptography, high-level reliability estimation flows for embedded processors, generalization of classic linear algebra kernels, and multilayered coarse-grained reconfigurable architecture. He is also a Series Editor of the Springer book series on *Computer Architecture and Design Methodologies*. His research in the area of emerging technologies has been covered by major news outlets across the world, including *Asian Scientist*, *The Straits Times*, and *The Economist*.

Dr. Chattopadhyay is a member of ACM. He received the Borcher's Plaque from RWTH Aachen for outstanding doctoral dissertation in 2008 and the nomination for the Best IP Award in the ACM/IEEE Design Automation and Test in Europe (DATE) Conference 2016 and the Best Paper Award in the International Conference on VLSI Design 2018. He regularly serves in the TPCs of top conferences and reviews journal/conference articles and presented multiple invited seminars/tutorials in prestigious venues.

Swaroop Ghosh (M'08–SM'13) received the B.E. degree (Hons.) from IIT Roorkee, Roorkee, India, the M.S. degree from the University of Cincinnati, Cincinnati, OH, USA, and the Ph.D. degree from Purdue University, West Lafayette, IN, USA.

He was a Senior Research and Development Engineer with Advanced Design, Intel Corp., Hillsboro, OR, USA, where his research was focused on low power and robust embedded memory design in scaled technologies. He was with the Faculty of the University of South Florida, Tampa, FL, USA. He is currently an Assistant Professor with the School of Electrical Engineering and Computer Science, Penn State University, State College, PA, USA. His current research interests include low-power circuits, hardware security, quantum computing, and digital testing for nanometer technologies.

Dr. Ghosh is a Senior Member of the National Academy of Inventors (NAI) and an Associate Member of Sigma Xi. He was a recipient of the Intel Technology and Manufacturing Group Excellence Award in 2009, the Intel Divisional Award in 2011, the Intel Departmental Awards in 2011 and 2012, the USF Outstanding Research Achievement Award in 2015, the College of Engineering Outstanding Research Achievement Award in 2015, the DARPA Young Faculty Award (YFA) in 2015, the ACM SIGDA Outstanding New Faculty Award in 2016, the YFA Director's Fellowship in 2017, the Monkowsky Career Development Award in 2018, the Lutron Spira Teaching Excellence Award in 2018, and the Dean's Certificate of Excellence in 2019. He has served on the Technical Program Committees of ACM/IEEE conferences, such as Design Automation Conference (DAC), International Conference on Computer Aided Design (ICCAD), Custom Integrated Circuits Conference (CICC), Design Automation and Test in Europe (DATE), International Symposium on Low Power Electronic Design (ISLPED), Great Lakes Symposium on Very Large Scale Integration (GLSVLSI), Nanoarch, and International Symposium on Quality Electronic Design (ISQED). He has served as the Program Chair of the DAC Ph.D. Forum in 2016 and ISQED in 2019 and the Track (Co)-Chair of ISQED from 2016 to 2017, ISLPED from 2017 to 2018, and CICC from 2017 to 2019. He has served as an Associate Editor for the IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—PART I: REGULAR PAPERS from 2014 to 2015 and as a Senior Editorial Board Member for the IEEE JOURNAL ON EMERGING AND SELECTED TOPICS IN CIRCUITS AND SYSTEMS (JETCAS) from 2016 to 2018. He has served as the Guest Editor for the IEEE JETCAS from 2015 to 2016 and the IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS from 2018 to 2019. He has been serving as an Associate Editor for the IEEE TRANSACTIONS ON COMPUTER-AIDED DESIGN OF INTEGRATED CIRCUITS AND SYSTEMS since 2019. He is also a Distinguished Speaker of the ACM.

Wayne Burleson (S'87–M'89–SM'01–F'11) received the B.S. and M.S. degrees in electrical engineering and computer science from the Massachusetts Institute of Technology, Cambridge, MA, USA, in 1983, and the Ph.D. degree in ECE from the University of Colorado at Boulder, Boulder, CO, USA, in 1989.

He has been a Professor of Electrical and Computer Engineering with the University of Massachusetts Amherst, Amherst, MA, USA, since 1990. From 2012 to 2017, he was a Senior Fellow with AMD Research, Boston, MA, USA. He has been a Custom Chip Designer and a Consultant in the semiconductor industry with VLSI Technology, San Jose, CA, USA; DEC, Maynard, MA, USA; Compaq/HP, Shrewsbury/Hudson, MA, USA; Intel, Shrewsbury/Hudson, MA, USA; Rambus, Sunnyvale, CA, USA; and AMD, Boston. He was a Visiting Professor with the École Nationale Supérieure des Télécommunications, Paris, France, from 1996 to 1997; the Laboratory of Informatics, Robotics and Microelectronics of Montpellier, Montpellier, France, in 2003; and the École Polytechnique Fédérale de Lausanne, Lausanne, Switzerland, from 2010 to 2011. He develops and teaches courses in VLSI design, embedded systems, and security engineering. He has authored over 200 refereed publications in these areas. His current research interests include the general area of VLSI, including circuits and CAD for low-power, long interconnects, clocking, reliability, thermal effects, process variation, noise mitigation, hardware security, reconfigurable computing, content-adaptive signal processing, radio frequency identification, and multimedia instructional technologies.

Debdeep Mukhopadhyay (M’13–SM’17) received the B.Tech., M.S., and Ph.D. degrees from IIT Kharagpur, Kharagpur, India.

He was an Associate Professor with IIT Kharagpur; a Visiting Scientist with Nanyang Technological University, Singapore; a Visiting Associate Professor with New York University Shanghai, Shanghai, China; an Assistant Professor with IIT Madras, Chennai, India; and a Visiting Researcher with the New York University Tandon School of Engineering, New York, NY, USA. He is currently a Full Professor with the Department of Computer Science and Engineering, IIT Kharagpur, where he initiated the Secured Embedded Architecture Laboratory (SEAL), with a focus on embedded security and side-channel attacks. He has recently incubated a start-up on hardware security, ESP Pvt., Ltd., IIT Kharagpur. His books include *Fault Tolerant Architectures for Cryptography and Hardware Security* (Springer), *Cryptography and Network Security* (McGraw Hills), *Hardware Security: Design, Threats, and Safeguards* (CRC Press), and *Timing Channels in Cryptography* (Springer). He has authored more than 150 articles in peer-reviewed conferences and journals and has collaborated with several Indian and foreign organizations. His current research interests include cryptography, hardware security, and VLSI.

Dr. Mukhopadhyay was a recipient of the prestigious Swarnajayanti DST Fellowship from 2015 to 2016, the Young Scientist Award from the Indian National Science Academy, and the Young Engineer Award from the Indian National Academy of Engineers. He is the Young Associate of the Indian Academy of Science. He was also awarded the Outstanding Young Faculty Fellowship by IIT Kharagpur in 2011 and the Techno-Inventor Best PhD Award by the Indian Semiconductor Association. He has been on the program committees of several top international conferences. He is also an Associate Editor of the International Association of Cryptologic Research (IACR) *Transactions of Cryptographic Hardware and Embedded Systems* (CHES), *Journal of Hardware and Systems Security*, *Journal of Cryptographic Engineering* (Springer), and the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY (IEEE TIFS). He has given several invited talks in industry and academia, including tutorial talks at premier conferences, such as CHES, Workshop on Information Forensics and Security (WIFS), and Very Large Scale Integration Design Conference (VLSID).