Digital Object Identifier 10.1109/TETC.2017.2738978

Guest Editors Introduction: Security of Beyond CMOS Devices: Issues and Opportunities

SWARUP BHUNIA, AN CHEN, OZGUR SINANOGLU, AND JASON M FUNG

Aggressive scaling of CMOS in the quest of smaller and faster transistors has brought us into the sub 10-nm technology era with the end of CMOS roadmap in sight. Number of alternative nanoscale devices – both silicon and non-silicon – with interesting switching characteristics have come onto the horizon. They promise to replace CMOS as computing and/or information carrier devices. Effective combination of innovative device structures with fundamental physical properties of materials and possibly entirely new state variables (e.g., mechanical state, electron spin) to represent information give rise to attractive functional properties of these nanoscale devices. These devices, however, primarily have been studied at different levels – from device physics to circuits and architecture – from the perspective of traditional device parameters – e.g., performance, power, reliability, non-volatility, and manufacturability. Security implications for these emerging nanoscale devices is an important and integral topic in system design which has not received adequate attention by the researchers.

These devices are poised to make profound impact in the design of secure information processing systems by creating new attack modalities, changing the effectiveness of current attack models and countermeasures, and by enabling new approaches to secure designs that leverage their unique characteristics. In order to provide a foundation for secure electronics and computing in the nanoscale era, we need to develop a deep understanding of the impact of nanoscale device characteristics to higher layers of design abstraction, where threat models and security properties are meaningfully defined. On one hand, we need to understand the device physics and operation of emerging devices as well as security primitives and attack models on the other. Such understanding will lead to the development of circuit-compatible models for these devices and design/analysis of common security primitives such as Physical Unclonable Functions (PUFs), Random Number Generators (RNGs), anti-cloning circuits, aging sensors, and cryptographic circuits. Furthermore, it will enable us to analyze the efficacy of existing attacks, such as side-channel attacks, aging attacks, counterfeiting, hardware intellectual property (IP) piracy, hardware Trojan attacks etc., and to discover unprecedented attack modalities. Finally, new defense mechanisms (e.g., new design of security primitives or more powerful cryptographic solution) may be enabled by the unique characteristics of nanoscale devices. With these observations in mind, this special issue aims at comprehensively covering security issues with beyond-CMOS devices and emerging security solutions for systems built with these devices.

It is our great pleasure to publish this special issue on security issues and opportunities for emerging post-CMOS nanoscale devices. This special issue contains the following four high-quality papers on diverse topics in nanoscale device security. Technical contributions in these papers range from security analysis for emerging devices to exploring design of new security primitives with them. We are extremely happy to choose these articles with distinctive contribution for this issue.

(1) (260) "Performance Enhancement of a Time-Delay PUF Design by Utilizing Integrated Nanoscale ReRAM Devices", by K. Beckmann *et al.*
(2) (265) "Timing Attack and Countermeasure on NEMS Relay Based Design of Block Ciphers", by B. Mazumdar *et al.*
(3) (278) "Univariate Power Analysis Attacks Exploiting Static Dissipation of Nanometer CMOS VLSI Circuits for Cryptographic Applications", by G. Scotti *et al.*
(4) (291) "Tunnel FET Current Mode Logic for DPA-Resilient Circuit Designs", by Y. Jin *et al.*

We believe the collection of articles in this special issue will help advance the security theory of nanoscale devices and stimulate interest for further research in this important topic. The selected articles are expected to answer some of the key questions in nanoscale security, as follows:

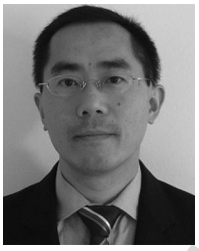
- What new attack models will emerge in the nanoscale era?
- How can we project the characteristics of nanoscale devices to system security properties?
- How effective are the existing countermeasures against known attack models?
- Will emerging devices provide new opportunities for building security primitives or countermeasures against various hardware security issues (e.g., side-channel attacks, Trojan attacks, IP piracy, etc.)?

We sincerely hope that you enjoy reading this special issue, and would like to thank all authors and reviewers for their tremendous efforts and contributions in producing these high-quality articles. We also take this opportunity to thank the *IEEE Transactions on Emerging Topics in Computing (TETC)* Editor-in-Chief (EIC) Prof. Fabrizio Lombardi,

Associate Editor Prof. Ramesh Karri, the editorial board, and the entire editorial staff for their guidance, encouragement and assistance in delivering this special issue.

SWARUP BHUNIA
University of Florida
swarup@ece.ufl.edu
AN CHEN
Semiconductor Research Corporation (SRC), An.C
hen@src.org
OZGUR SINANOGLU
New York University
os22@nyu.edu
JASON M. FUNG
Intel
jason.m.fung@intel.com

SWARUP BHUNIA is a preeminence professor of cybersecurity and Steven Yatauro endowed faculty fellow of computer engineering with University of Florida, Florida. Earlier he was appointed as the T. and A. Schroeder associate professor of Electrical Engineering and Computer Science with Case Western Reserve University, Cleveland, ohio. He has over twenty years of research and development experience with 250+ publications in peer-reviewed journals and premier conferences and six authored/edited books. His research interests include hardware security and trust, adaptive nanocomputing and novel test methodologies. He is co-founding editor-in-chief of the Springer *Journal on Hardware and Systems Security*. He has been serving as an associate editor of the *IEEE Transactions on CAD*, the *IEEE Transactions on Multi-Scale Computing Systems*, the *ACM Journal of Emerging Technologies*, and the *Journal of Low Power Electronics*; served as guest editor of the *IEEE Design & Test of Computers* (2010, 2013) and the *IEEE Journal on Emerging and Selected Topics in Circuits and Systems* (2014). He has served as general chair of HOST 2017, program chair of IMS3TW 2011, NANOARCH 2013, VDAT 2014, and HOST 2016, and in the program committee of several IEEE/ACM conferences. Dr. Bhunia received his PhD from Purdue University on energy-efficient and robust electronics. He is a senior member of the IEEE.



AN CHEN received the PhD degree in electrical engineering from Yale University, in 2004. He is on assignment from the IBM Corporation to serve as the executive director of the Nanoelectronics Research Initiative (NRI), and is based at the Almaden Research Laboratories in San Jose, California. The NRI supports university-based research on future nanoscale logic devices to replace the CMOS transistor in the 2020 timeframe. He started working on emerging memory technologies with Spansion LLC. In 2007, he joined AMD as a full-time assignee to the Nanoelectronics Research Initiative (NRI) program with SRC. He continued working on beyond-CMOS devices with the NRI and STARnet programs at GLOBALFOUNDRIES, which separated from AMD in 2009. He is also a memory Tech Lead responsible for research collaborations with industry consortia and partners on emerging memories. Since 2011, he has been the chair of the Emerging Research Device (ERD) group of the International Technology Roadmap for Semiconductors (ITRS). He has published 38 first-author and 7 co-author papers in peer-review journal and conference proceedings. He holds 16 issued U.S. patents and 4 pending applications. He has presented more than 20 contributed talks and more than 30 invited talks and panel discussions in conferences. He is the lead editor of "Emerging Nanoelectronic Devices" (Wiley, 2015) and has contributed chapters to four books. He is on the Advisory Boards of U. Nebraska Lincoln MRSEC center and U. Florida Nanoscale Security MURI program, and has also served in the Technical Advisory Board of several SRC programs and thrusts. He is a senior member of the IEEE.

OZGUR SINANOGLU received the BS degrees, one in electrical and electronics engineering and one in computer engineering, both from Bogazici University, Turkey, in 1999. He received the MS and PhD degrees in computer science and engineering from University of California San Diego, in 2001 and 2004, respectively. He is an associate professor of electrical and computer engineering with New York University Abu Dhabi. He has industry experience at TI, IBM and Qualcomm, and has been with NYU Abu Dhabi since 2010. During the PhD, he won the IBM PhD fellowship award twice. He is also the recipient of the best paper awards at IEEE VLSI Test Symposium 2011 and ACM Conference on Computer and Communication Security 2013. His research interests include design-for-test, design-for-security and design-for-trust for VLSI circuits, where he has more than 160 conference and journal papers, and 20 issued and pending US Patents. Sinanoglu has given more than a dozen tutorials on hardware security and trust in leading CAD and test conferences, such as DAC, DATE, ITC, VTS, ETS, ICCD, ISQED, etc. He is serving as track/topic chair or technical program committee member in about 15 conferences, and as (guest) associate editor for IEEE TIFS, IEEE TCAD, ACM JETC, IEEE TETC, Elsevier MEJ, JETTA, and IET CDT journals. Prof. Sinanoglu is the director of the Design-for-Excellence Lab at NYU Abu Dhabi. His recent research in hardware security and trust is being funded by US National Science Foundation, US Department of Defense, Semiconductor Research Corporation, and Mubadala Technology.

JASON M. FUNG received the two BS degrees, one in computer science and mathematics and another in electrical and computer engineering, from Carnegie Mellon University, in 1997. He received the MS degree in electrical and computer engineering from Carnegie Mellon University, in 1998. He is a product security research manager with Intel's Security Center of Excellence (SeCoE). His motto "Ensure Technology Truly Enriches Lives" captures his passion on security and privacy. He is responsible for the security assurance and research strategy for Intel's device and modem SoC products that power PC clients, tablets, phones, Internet of Things, automotive, cellular communications, and more. Since joining Intel Corporation in 1998, he has led and contributed to many software and hardware programs involving architecture, development, validation, tools and methodologies, research, consultation, and engineering management. He has more than 12 years of hands-on experience in product security evaluation, penetration testing, risk management, pathfinding and research. He is very passionate in advancing product security and privacy research within Intel. He serves in the Planning Committee and/or Technical Program Committee for several internal conferences. For example, he established the "Security, Privacy and Safety" track at the Software Professional Conference, a premier internal conference attended by thousands of technologists at 15 work sites around the world, and has been serving as the Track Chair since 2013. He established SeCoE's Security Research Initiative that sponsors multi-year research projects to foster innovations on key strategic areas. Jason is also very active in academia collaboration, shaping research direction and student education on security. He received the Mahboob Khan Outstanding Liaison Award from Semiconductor Research Corporation (SRC) in 2016. He holds 3 issued US Patents and has over a dozen publications in premier IEEE/ACM and Intel internal conferences.