Guest Editorial
Special Issue on Secure and Trustworthy Computing

OZGUR SINANOGLU, New York University Abu Dhabi, UAE
RAMESH KARRI, New York University, New York

There is a growing concern regarding the trustworthiness and reliability of the hardware underlying all information systems on which modern society is reliant. Trustworthy and reliable semiconductor supply chain, hardware components, and platforms are essential to all critical infrastructures including financial, healthcare, transportation, and energy. Traditionally, the information systems underlying all critical infrastructures were being protected—specifically the authenticity, integrity, and confidentiality of the information was being ensured—using security protocols implemented in software running on hardware platforms that were assumed to be trustworthy and reliable.

However, this assumption is no longer true; an increasing number of attacks are being reported on the hardware root of trust [https://isis.poly.edu/esc/2014/index.html]. Since 2008, NYU has been organizing the annual Embedded Security Challenge (ESC) to demonstrate the ease and feasibility of hardware-based attacks on information systems. As part of this annual event, ESC2014 challenged the hardware security and emerging technologies communities to investigate hardware-based attacks and hardware-based security primitives rooted in emerging technologies according to the tutorial papers on this topic [Rajendran et al. 2012, 2015].

ESC 2014 had three phases [https://isis.poly.edu/esc/2014/index.html]. In phase 1, 14 teams submitted a 2-page proposal that described an emerging technology, the structure and operation of the security primitives that exploited the unique characteristics of the chosen emerging technology, the threat model that the security primitives target, the security metrics used to evaluate the security primitives and applications of the developed security primitives. Ten promising proposals were down-selected for Phase 2 of ESC 2014. In this phase, participants developed and evaluated their emerging technology-based security primitives. In the ESC 2014 finals held at NYU in November 2014, as part of the annual NYU Cyber Security Awareness Week, the ten finalists demonstrated and presented their security primitives and submitted a final report.

Examples of security primitives included, but were not limited to, cryptographically secure pseudo-random number generators, public-key and private-key cryptography, one-way hash functions, and physical unclonable functions. Emerging technologies that were considered include: graphene transistors, atomic switches, memristors, Mott field effect transistor, spin FET, all-spin-logic, spin-wave devices, orthogonal spin-transfer random access memory, magneto-resistive random access memory, spintronic devices, nanomagnets, nano-electromechanical switches and phase-change memory. The finalists included Case Western Reserve University, Rochester Institute of Technology, University of Central Florida, University of Illinois at Urbana-Champaign, University of

Authors' addresses: O. Sinanoglu, New York University Abu Dhabi (NYUAD) Campus, Saadiyat Island, Abu Dhabi, United Arab Emirates, PO Box 129188; email: ozgursin@nyu.edu; R. Karri, 6 Metrotech Center, Brooklyn, NY 11201; email: rkarri@nyu.edu.

1550-4832/2016/06-ART1
DOI: http://dx.doi.org/10.1145/2898433

New Hampshire, University of Pittsburgh, University of South Florida (two teams), University of San Antonio, and Vanderbilt University. These reports can be downloaded from https://isis.poly.edu/esc/2014/reports.html.

All participants of ESC 2014 and the community at-large were invited to submit papers to the *ACM Journal on Emerging Technologies in Computing Systems* special issue on secure and trustworthy computing. A specific focus of this special issue is the impact and implications of emerging nanoscale technologies on hardware-based security. On one hand, physical properties offered by emerging nanoscale technologies may present an opportunity to create security primitives that is not possible or is difficult to implement with existing CMOS-based technologies. On the other hand, while they may improve certain aspects such as area, performance, and power, these emerging technologies may in turn introduce additional vulnerabilities that need to be studied and mitigated before deploying the defenses in security-critical applications.

This special issue includes four articles on emerging nanotechnologies for security. The first article is by the winners of the ESC 2014 nanosecurity challenge. This article from the University of South Florida studies nanomagnets and the security implications of the geometric and resistive variations in nanomagnet-based magnetic RAMs. The second article, a collaborative work by the ESC 2014 runners-up University of Central Florida and their EPFL and University of Notre Dame collaborators, investigates the unique properties of emerging Silicon Nanowire FETs and GrapheneSymFets in building security primitives for applications to lay out camouflaging, leading to an Intellectual Property (IP) protection methodology. The next article is from the ESC 2014 third-place team from the University of South Florida. This article shows how one can leverage the variability and randomness induced by the emerging spintronics in creating a robust, unclonable, and unpredictable physical unclonable function. The final article by Politecnico di Torino, LIRMM, and Universita di Napoli also investigates the security implications of spintronic devices.

The second half of the special issue includes five articles in the general area of CMOS-based hardware security. The first article by University of Connecticut researchers provides a comprehensive survey on reverse engineering, which is a major threat that enables various attacks, ranging form fault injection to cloning, counterfeiting, and tampering. The next article from researchers from LIRMM and ENSMSE is a comprehensive study on laser injection methods and the resulting fault attacks in the context of cryptographic ICs. This is followed by an article from Politecnico di Milano and STMicroelectronics, which presents fault attacks on cryptoprimitives to recover the embedded secret keyand a countermeasure to mitigate the attack. The next article is on CMOS-based random number generator and a silicon demonstration of the random number generator. Finally, the last article is on real-time anomaly detection via machine learning in multicore Network-on-Chips (NOCs). This article shows that attacks launched through the routers on the NOC, such as traffic diversion and route looping, can be detected in real time using these techniques.

We hope that this special issue will trigger research at the intersection of security and emerging nanotechnologies. Beyond this special issue, it is clear that hardware security has emerged as a key field. IC design, automation, and test communities are beginning to address the associated challenges by developing impactful solutions. Leading conferences, such as IEEE/ACM HOST, IEEE/ACM DAC, IEEE ICCAD, ASP-DAC, IEEE ITC, IEEE VTS, and IEEE/ACM ICCD, have embraced hardware security as a focus area. Leading journals, including ACM JETC (focus: emerging security technologies), ACM TODAES (focus: security-aware CAD), IEEE TCAD (focus: security-aware CAD Design and Test), IEEE TETC (focus: emerging security technologies), and IEEE TVLSI (focus: secure VLSI design), have published special issues on these topics and

are routinely publishing papers on these topics. Consistent with this trend, ACM JETC welcomes high-quality articles on hardware security throughout the year.

The guest editors would be remiss, if we didn't acknowledge the key contributors to this special issue, especially the authors. Since this is an emerging area, there were many more articles than qualified reviewers. Our heartfelt thanks to all the reviewers. Finally, a sincere thank you to the leadership of ACM JETC, including the outgoing Editor-in-Chief Prof. Krish Chakrabarty, the incoming Editor-in-Chief Prof. Yuan Xie, JETC administrator Ms. Rhonda Adams, and the ACM publication staff for managing the article submissions, reviews, and the special issue in general.

REFERENCES

J. Rajendran, R. Karri, J. B. Wendt, M. Potkonjak, N. McDonald, G. S. Rose, and B. Wysocki. 2012. Nanoelectronic solutions for hardware security. Retrieved from https://eprint.iacr.org/2012/575.

J. Rajendran, R. Karri, J. B. Wendt, M. Potkonjak, N. McDonald, G. S. Rose, and B. Wysocki. 2015. Nano meets security: Exploring nanoelectronic devices for security applications. *Proc. IEEE*, 103, 5 (May 2015), 829–849.

A. Detrano and V. Jyothi. 2014. Embedded Security Challenge Description. https://isis.poly.edu/esc/2014/index.html.

A. Detrano and V. Jyothi. 2014. Embedded Security Challenge Reports. https://isis.poly.edu/esc/2014/reports.html.