IEEE TRANSACTIONS ON
EMERGING TOPICS
IN COMPUTING

Digital Object Identifier 10.1109/TETC.2014.2318951

Special Issue on Emerging Nanoscale Architectures for Hardware Security, Trust, and Reliability: Part 1

THERE is an increasing concern involving the security, trust, and reliability of the hardware underlying the information systems on which modern society is reliant for mission-critical and safety-critical functions. Secure, trustworthy and reliable hardware components, and platforms and supply chains are vital to all domains, including financial, healthcare, transportation, energy, and the national defense. Traditionally, authenticity, integrity, and confidentiality of information were being protected with security protocols in software with the underlying hardware assumed to be secure, trustworthy, and reliable. However, this assumption is no longer true with an increasing number of attacks being reported on the hardware root of trust. Whereas security, trust, and reliability risks are better understood in software, understanding and addressing threats to the hardware root of trust are a critical emerging challenge and the focus of this special issue.

This special issue has nine papers by leading research groups in the emerging area of hardware security and trustworthy hardware. Seven of them will appear in this volume and the remaining two will appear in a subsequent volume.

The first paper ''On-Chip Nanoscale Capacitor Decoupling Architectures for Hardware Security'' demonstrates the use of on-chip nMOS gate capacitors as intermediate power storage elements to decouple the power supply from internal low-power modules processing sensitive data and in turn thwart differential power analysis.

The special issue has three papers on various aspects of the hardware-based security primitive called physically unclonable function (PUF). The paper entitled ''Processor-Based Strong Physical Unclonable Functions With Aging-Based Response Tuning'' proposes a lightweight PUF based on the timing difference introduced into processor architectures. First, it builds a PUF by using the timing differences in ALUs on two distinct processor cores. The cores are then intentionally aged to tune the statistical properties of the baseline 2-core PUF. The paper ''A PUF Based on Transient Effect Ring Oscillator and Insensitive to Locking Phenomenon'' describes a new ring oscillator PUF that uses the number of transitions in an RO loop structure to generate unique chip identifiers. This PUF structure can also be used for random number generation. The paper ''Robust and Reverse-Engineering Resilient PUF Authentication and Key-Exchange by Substring Matching'' presents PUF-based authentication and key exchange protocols that matches only a random subsets of the PUF response strings. This paper analyzes the increase in security of these protocols.

The paper entitled ''Test versus Security: Past, Present, and Future'' summarizes the ten years of research in the area of security implications of VLSI Testing. Design-for-Testability structures are introduced into designs to improve the testability of VLSI circuits. However, an attacker can extract secret information stored on the chip using this test infrastructure. This paper is comprehensively surveys the state of the art in scan testing based attacks with a particular focus on hardware implementations of symmetric and public-key cryptography.

The paper ''Reverse Engineering Digital Circuits Using Structural and Functional Analyzes'' reports a reverse engineering method on digital circuits based on a set of algorithms in order to identify functional units from a flattened netlist. The final paper of this volume, ''Fabrication Attacks: Zero-Overhead Malicious Modifications Enabling Modern Microprocessor Privilege Escalation'' presents and analyzes two attacks that escalate the privilege during a microprocessor's operation. If an attacker can escalate the privilege, then the microprocessor is compromised and can be used maliciously (e.g., leak sensitive data). The attacks were emulated in software and hardware.

The first paper of volume 2 ''Obtaining Statistically Random Information from Silicon Physical Unclonable Functions'' presents approaches to improve the randomness of silicon PUFs. Most importantly, this technique can apply to and improve the security of all silicon PUFs.

The second and final paper of volume 2 entitled ''A Combined Design-Time/Test-Time Study of the Vulnerability of Subthreshold Devices to Low Voltage Fault Attacks'' demonstrates that it is possible to inject faults useful for differential fault analysis into a 65-nm implementation of the Advanced Encryption Standard (AES) operating in the subthreshold voltage range. This attack highlights the vulnerability of such low power implementations of AES potentially used in RFIDs.

RAMESH KARRI, *Guest Editor*
New York University
New York, USA
http://eeweb.poly.edu/karri/

MIODRAG POTKONJAK, *Guest Editor*
Computer Science Department, UCLA
Los Angeles, USA
http://www.cs.ucla.edu/~miodrag/

Ramesh Karri (M'92) received the B.E. degree in electronics and communications engineering from Andhra University, Visakhapatnam, India, in 1985, the M.S. degree in computer science from the University of Hyderabad, Hyderabad, India, in 1988, the M.S. degree in computer engineering and the Ph.D. degree in computer science from the University of California at San Diego, La Jolla, CA, USA, in 1992 and 1993, respectively. He is a Professor with the Electrical and Computer Engineering Department, New York University, New York, NY, USA. His research interests include trustworthy hardware design and the interaction between security and reliability. He has authored over 150 conference and journal articles in these areas. He was a recipient of the NSF CAREER Award and the Alexander Humboldt Fellowship. He is serving as the General Chair of the 2013 IEEE Symposium on Hardware-Oriented Security and Trust (HOST), the General Co-Chair of the 2013 IEEE Symposium on Nanoscale Architectures, and the 2013 IEEE Symposium on Defect and Fault Tolerant (DFT) VLSI, and was the Program Chair of the 2012 HOST and the 2012 DFT. He organizes the Annual Embedded Systems Challenge (ESC) to build a security mindset in hardware and embedded system designers. ESC is a red team blue team activity. He is a Co-Founder of the Trusthub, a community research and outreach infrastructure, i.e., the go to source for all things hardware and embedded systems security. He is an Associate Editor of the *IEEE Transactions on Information Forensics and Security*, the *IEEE Transactions on Computer Aided Design*, and the *ACM Journal of Emerging Technologies in Computing Systems*. He has served or is currently serving on several conference program committees (including Program and General Chair of HOST and 2014 DAC Security Track Co-Chair). He has organized or is organizing special sessions of conferences and special issues of journals in the area of hardware trust, including an upcoming special issue of the Proceedings of IEEE.

Miodrag Potkonjak (M'92) received the Ph.D. degree in electrical engineering and computer science from the University of California, Berkeley, CA, USA, in 1991. After spending four years with the Communication and Computation Research Laboratory, NEC Labs, Princeton, NJ, USA, he joined Computer Science Department with the University of California at Los Angeles (UCLA), CA, USA, where he has been a Professor since 2000. He received the NSF CAREER and OKAWA Foundation Award.

He received the TRW/School of Engineering and Applied Science at UCLA Excellence in Teaching Award and a number of Best Paper Awards and nominations including best papers at the 2001 International Conference on Mobile Computing and Networking and the 2013 International Workshop on Power and Timing Modeling, Optimization and Simulation. He was involved in anthologies of best papers in leading conferences and journals. According to Microsoft Libra, one of his papers is among top five most cited papers all times in both computer architecture and hardware and embedded and real-time systems fields. He has authored two books and more than 400 papers in leading communication, CAD and VLSI design, embedded systems, real-time systems, computational sensing, and security journals and conferences. He holds 45 patents and has more than 50 additional patent applications.

His current research interests are focused on semantic analysis, computational sensing, ultra low power systems, low latency computation and communication, embedded systems, security, privacy and trust, systems, physical, chemical, biological, and social security. He has created the first watermarking, fingerprinting, and metering techniques for integrated circuits, and approaches for remote trusted sensing and trusted synthesis and compilation using untrusted tools. His watermarking-based intellectual property protection research formed a basis for the Virtual Socket Initiative Alliance standard.