Guest Editorial
Integrated Circuit and System Security

HARDWARE security is a research area that is simultaneously mature (covert and side channels, security of cryptographic systems, and watermarking have been extensively explored) and rather early in its development (physical, unclonable functions, hardware Trojan horses, and other primitives and vulnerabilities are beginning to be explored). Moreover, hardware security has a rich yet complicated relationship to classical algorithmic cryptography and security. On one hand it tries to complement this established field. On the other hand, it competes with this field both in terms of outperforming on classical security problems and solving previously unsolvable problems.

Mindful of the pitfalls and opportunities, our primary objective in organizing this Special Issue was to provide additional impetus for research in hardware security. Currently, the field is heavily dominated by testing, CAD, and IC researchers. We hope that researchers from other security fields will find the problems and the proposed solutions published here both interesting and important.

The proper way to structure research and development tasks of the overall hardware-based security fields starts with the identification of security primitives, protocols, and amplifiers. The primitives include watermarking and physical unclonable functions (PUFs). There have been a number of hardware security protocols for hardware and software metering. However, these protocols were monolithic and did not take advantage of the modular research structures. Koushanfar's conference paper on IC digital rights management was the first work that created security protocols using hardware security primitives such as PUFs. The key idea is to use ramifications of process variations that make each chip unique. The IC activation requires an activation key from the designer. Therefore, fabrication of nonauthorized ICs is prevented. The Special Issue version of the paper focuses on establishing sound theoretical proofs that a broad and realistic set of attacks is not feasible.

This paper is related to two groups of papers. One group consists of a single paper on FPGA DRM. The second group consists of three papers that provide theoretical treatment of hardware security issues. Members of the COSIC research group at Katholike Universiteit Leuven authored the FPGA DRM paper. The paper presents one of the first protocols for a pay-per-use licensing technique for hardware IP cores in the state-of-the-art SRAM-based FPGA. The authors present a security protocol that requires participation of a trusted third party while introducing a small implementation overhead. We can expect an increased interest in developing and deploying these types of security protocols; over 100 000 FPGA unique designs are already created this year.

The first paper with a strong theoretical component is titled "Proof-Carrying Hardware Intellectual Property: A Pathway to Trusted Module Acquisition" and authored by Eric Love, *et al.* This is the second effort to develop techniques for checking the security properties of hardware specified in HDL code. The first technique presented at DAC 2010 used the notion of a fully specified design where all resources are used by the specification at all times. The starting point of the new technique is the popular proof-carrying code technique. The proposed system automatically detects malicious HDL via formal verification of the security policies upon which the code provider and the customer agree.

Covert channels are one of the oldest and most studied system security attacks. The NRL Network Pump is a popular and widely advocated mechanism to reduce the impact of covert channels in a multilevel secure system. However, until now, the NRL network pump was not exactly characterized. The team from the University of Illinois at Urbana and Naval Research Laboratory used information theoretic analysis to establish the conditions under which covert channels can be closed using the NRL network pump.

Advanced Encryption Standard (AES) is the most popular and widely used private-key cryptography primitive. It has been recognized quite early (in 1996) that any cryptographic implementation (including the hardware implementations of AES) can be compromised using side channels including timing, power, and electromagnetic radiation. In addition, AES secret keys can be leaked by intentional injection of computational faults. Two excellent papers further advance the state-of-the-art of this type of attack. The first is titled "Improved Differential Fault Analysis on AES Key Schedule." The author, C. H. Kim, has proposed a novel fault attack on AES by injecting faults during the key schedule. Using the proposed method, the secret key of the AES-128/192/256 is analyzed with lowest cost in terms of number of faults and steps of brute-force search with respect to the previously published literature. Fault analysis on the AES key schedule is more difficult than that on the state because errors propagate on both the key and the state data. The second reason is that fault analysis on the key schedule is harder to protect. While fault analysis on the state can be prevented with state randomization methods, fault analysis on key schedule cannot be prevented using that method. A research team from The University of Electro-Communications, Tokyo authored the second paper. The paper has a theoretical component that explains why fault sensitivity analysis is possible against AES hardware implementations that are already resistant to the differential fault analysis. The paper also proposes several security measures against the proposed fault sensitivity analysis.

Authentication is one of the first and canonical security tasks. It is closely related to numerous other security tasks such as Identification, hardware, software and data metering, and data

Digital Object Identifier 10.1109/TIFS.2011.2180833

verification. In hardware security, it has even more applications and aspects due to its close relationship to the physical properties of devices. A team from the U.S. Air Force Institute of Technology at Wright-Patterson AFB, OH, presents a new RF distinct native attribute fingerprinting technique to create a multifactor-authentication approach demonstrating the use of a combination of measurements and data processing using statistical techniques.

We wish to express our gratitude to the authors of accepted papers for their high-quality research contributions and clearly written manuscripts. We also thank the reviewers for their detailed, constructive, and timely comments that further improved the importance of these contributions. The competition for inclusion in the Special Issue was intense and space is always limited. Thus, we wish to thank the authors of all submitted manuscripts that have not made it to these pages. We appreciated the opportunity to review your efforts and are enthusiastic about the work in which you are engaged. We also wish to thank Prof. Nasir Memon, Editor-in-Chief of IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, for his support, guidance, and occasional prodding. Finally, we gratefully acknowledge the outstanding logistical support of all IEEE staff and in particular Deborah Tomaro and Rebecca Wollman.

MIODRAG POTKONJAK, *Lead Guest Editor*
Computer Science Department
UCLA
Los Angeles, CA 90095-1596 USA

RAMESH KARRI, *Guest Editor*
Department of Electrical and Computer Engineering
Polytechnic Institute of New York University
Brooklyn, NY 11201 USA

INGRID VERBAUWHEDE, *Guest Editor*
COSIC/ESAT
K.U. Leuven
Heverlee, B-3001 Belgium

KOUICHI ITOH, *Guest Editor*
Secure Computing Laboratories
Fujitsu Laboratories Ltd.
Kawasaki, Kanagawa 211-8588 Japan

Miodrag Potkonjak received the Ph.D. degree in electrical engineering and computer science from the University of California, Berkeley in 1991. He is a Professor in the Department of Computer Science at UCLA. He published over 350 papers in leading CAD, VLSI design, and security journals and conferences. He holds 15 patents. His current research interests are focused on security and trust for synthesis and operation of integrated circuits and systems, physical, chemical, and biological security.

Ramesh Karri received the Ph.D. degree in computer science from the University of California, San Diego in 1993. He is a Professor in the Electrical and Computer Engineering Department, Polytechnic Institute of New York University, Brooklyn. He has published over 100 conference and journal articles in these areas. His research interests include trustworthy hardware and reliable nanoscale architectures. He is an Associate Editor of IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY and *ACM Journal of Emerging Technologies in Computing*.

Ingrid Verbauwhede received the Ph.D. degree from K.U. Leuven. She is a professor at K. U. Leuven and an adjunct professor at UCLA. Her research group is part of the Computer Security and Industrial Cryptography (COSIC) Laboratory. Embedded security is the focus of her research; it includes new technologies, circuits, architectures, and design methodologies for efficient and secure implementations of cryptography and security applications. She serves on the committees of leading conferences in hardware security.

Kouichi Itoh received the Ph.D. degree in engineering from Tokyo Institute of Technology in 2009. He is with Fujitsu Laboratories Ltd., where he has been involved in research and development of implementation of public-key and common-key cryptosystems and side channel attacks. He has published over 50 journal and refereed conference articles and holds over 10 patents and filed over 20 patents. He is an editor of *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*.