Call for Papers
IEEE Transactions on Information Forensics and Security
Special Issue on
Integrated Circuit and System Security

The ever increasing complexity of modern and emerging integrated circuit (IC) technologies matched with the ever decreasing controllability and observability, process variation, circuit aging, and other deep submicron technology effects have simultaneously created tremendous security vulnerabilities and exceptional security mechanisms. On the one hand, malicious attacks using approaches such as ghost circuitry, untrusted computer aided design tools, and side channel signal processing can easily break traditional security platforms. On the other hand, new mechanisms such as physically unclonable functions and their emerging hardware public key generalizations may be a basis for a variety of security protocols.

Hardware-based security is on the brink of a revolution and this special issue seeks to showcase the latest advances in state-of-the-art hardware security techniques and identify the most promising research frontiers in IC and system security. Its scope spans all aspects of IC and system security ranging from theoretical and conceptual foundations, synthesis, testing and verification, to modeling, signal analysis, signal processing, and optimization to case studies. The emphasis is on innovative and sound techniques with conceptual innovations that can scale to industrial strength implementations. Topics of interest include but are not limited to:

- Hardware security primitives (circuitry and mechanisms) including IDs, PUFs, PPUFs, public TRNGs, side channels, dual rail logic, controlled aging, IC conditioning, watermarking, fingerprinting, and obfuscation
- Hardware-based security protocols including DRM (IC metering, enabling and disabling), trust guarantees, authentication, privacy, hardware-based PKC, IP protection
- Hardware attacks: creation, detection, characterization, and compensation
- Forensics and reverse engineering (e.g. process, IC, models, algorithms)
- Computer aided design (CAD) techniques for IC and System Security
- Trusted synthesis and compilation using untrustworthy CAD tools
- Trusted hardware based system security
- Secure communication, storage, sensing, and actuation systems
- Impact of nano and other emerging technologies on hardware-based system security
- Hardware-supported primitives and protocols for operating systems and utility software
- Hardware-based physical, chemical, biological, medical security including digital locks, tools for detection of dangerous materials, secure and trustable sensing devices, and sensor networks.
- Hardware-based personal and social security devices and protocols

Manuscript Submission: Manuscripts are to be submitted according to the Information for Authors at http://www.signalprocessingsociety.org/publications/periodicals/forensics/forensics-authors-info/, using the IEEE online manuscript system, Manuscript Central. Papers must not have appeared elsewhere, and must not be in review elsewhere. All papers will be reviewed in accordance with the procedures of the IEEE Transactions.

Extended Submission Deadline (Firm Deadline): January 20, 2011
First Review: April 1, 2011
Revisions Due: May 1, 2011
Final Decision: June 1, 2011
Final Manuscript Due: July 1, 2011
Tentative Publication Date: December 2011

Guest Editors:
Miodrag Potkonjak, University of California, Los Angeles, miodrag@cs.ucla.edu
Ramesh Karri, Polytechnic Institute of New York University, rkarri@duke.poly.edu
Ingrid Verbauwhede, Katholieke University Leuven, Belgium, Ingrid.Verbauwhede@esat.kuleuven.be
Kouichi Itoh, Fujitsu Labs, Japan, kito@labs.fujitsu.com