IEEE Transactions on VLSI Systems

Call for Papers

Announcing a Special Issue in:

Securing IoT Hardware: Threat models and Reliable, Low-power Design Solutions

~~**Submission deadline: Dec 31, 2016**~~
Extended deadline: January 21, 2017

IEEE Transactions on VLSI invites manuscripts in the area of '*Securing IoT Hardware: Threat models and Reliable, Low-power Design Solutions*'.

The IEEE Transactions on VLSI Systems is published as a monthly journal under the co-sponsorship of the IEEE Circuits and Systems Society, the IEEE Computer Society, and the IEEE Solid-State Circuits Society. This special section is targeted towards hardware security of the internet-of-things (IoT).

It is well-acknowledged that for IoT, security of the underlying hardware is the key for safe and reliable operation. Unfortunately, no silver bullet has emerged that can deal with all forms of cyber threat related to IoT hardware. For example, IoT hardware can become increasingly vulnerable to attacks/threats due to globalization involved in the design supply chain. Long term device wear-out and/or transient faults, side channel information leakage, or intellectual property reverse engineering can be exploited to create security vulnerabilities. Some IoT systems – though not all are also power and cost sensitive. Standard crypto solutions are deemed expensive for both power and cost leading to demand for low-power design alternatives.

This special issue aims to present novel solutions for any problems related to IoT hardware, for example (but not limited to) in terms of security, threat models, reliability, low power design solutions and design parameter optimization.

Suitable topics (but not limited to) include:

Secured hardware for IoT	Reliable (in terms of thermal, power, device wear-out etc.) hardware for IoT	Trustworthy hardware for IoT
Anti-piracy methodologies for IoT hardware	Trojan secured IoT hardware	SEU/Transient fault secured hardware for IoT
Ownership abuse of IPs used IoT hardware	Ownership conflicts in IP: computational forensic engineering	Low power, high performance Design for IoT hardware

Manuscripts should conform to technical requirements of the Transactions on VLSI – they should be unpublished and original. Submissions that are extensions of previously published conference papers should have at least 30% in terms of new content excluding introduction and review of literature. Papers outside the scope of the special section will be moved automatically to regular section. This will also be true for papers that involve conflict of interest involving *both* guest editors.

Guest Editors:
Anirban Sengupta, Computer Science & Engineering, Indian Institute of Technology Indore, India
(Email: asengupt@iiti.ac.in)

Sandip Kundu, Electrical & Computer Engineering, University of Massachusetts, Amherst, USA
Email: kundu@umass.edu

Editor-in-Chief:
Krishnendu Chakrabarty, Computer Science, Duke University, USA
(Email: krish@duke.edu)

Submission Details:
All manuscripts must be submitted through the TVLSI ScholarOne site https://mc.manuscriptcentral.com/tvlsi-ieee.
Once you start the submission process in your Author Center, make sure to do the following:

1. Step 1/Type: Make sure to choose "Special Section"
2. Step 5/Special Section: Choose "Securing IoTHardware: Reliable and Low-Power Design Solutions" in the dropdown menu

Failure to choose both options will result in your manuscript being processed in the general pool

For more information on IEEE Transactions on VLSI Systems, please visit the following website:
http://tvlsi.egr.duke.edu/