IEEE Transactions on VLSI Systems

Call for papers

Special issue on: Security Challenges and Solutions with Emerging Computing Technologies

Submission deadline: January 10, 2019

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 issue is about security challenges and solutions with emerging computing technologies, including circuit design, architecture, automation and studies on vulnerabilities.

Multiple emerging computing technologies, based on, e.g., Graphene, Spintronics, Resistive RAM, Quantum Computing and others are being developed to enhance the capabilities of logic devices and circuits. The rapid growth in these technologies is synchronized with the decline of Moore's law, and thus promises to herald the era of Beyond CMOS technologies with a significant improvement in energy-efficiency, reliability, performance and manufacturability. These devices enable very different computing paradigms, e.g., neuromorphic computing, non-Boolean computing, and in-memory computing, thus making these platforms an interesting playground for circuit, and application-developers alike.

In this special issue, we are interested to put together the impact of these new technologies, especially novel circuits, on secure system designs.

For example, several of these devices are opening up new information side channels, which require careful analysis before using those as implementation platforms for cryptographic primitives. From another perspective, phenomenon like cross-talk in these devices can threaten well-founded counter-measures like masking which assume independence of the mask values. Likewise, fault tolerance of these devices in the context of security needs a fresh evaluation. On the other hand, for many practical use cases like IoT/CPS, and emerging cryptographic standards like post-quantum cryptography, the security kernels and countermeasures need to be designed with stringent constraints on area/energy footprints. Therefore, identifying suitable design choices and adapting them to different applications in the IoT/CPS context is a need of the hour. In essence, both the design and attack paradigms for secure systems are blended with the emergence of new computing technologies, which will be covered in this special issue.

This special issue aims to serve as a key milestone towards the emergence of the cross-disciplinary theme encompassing security and emerging computing technologies.

The topics of interest include, but not limited to, the following.

Security Kernel Design:

- Device/Circuit perspectives, co-design for emerging technologies for security systems
- Post-Quantum Cryptography on Beyond-CMOS technologies

- Modelling, Implementation, Testing and Benchmarking of Physically Unclonable Functions using Emerging Technologies
- Beyond Von Neumann architectures: (neuromorphic, in-memory computing) and their implication on the design, and resilience of security accelerators
- Practical Implementations and Case Studies using emerging technologies for security applications
- Novel technology/circuit-level Attack Resistance Mechanisms
- Chain-of-Trust Design in Emerging Computing Technologies
- Fundamental enhancements in neuromorphic computing to support security/trust mechanism design

Quantum-Enabled Attacks, Modelling Attacks, Information Leakage and Side-Channel Attack:

- New passive/active side channel attacks on circuits built using emerging computing technologies
- Modelling of Information Leakage for emerging computing technologies and Side-Channel Attacks
- Fault attacks for emerging technologies using novel equipment
- Novel Quantum-enabled attacks on cryptosystems and estimations
- Machine Learning Attacks on secure systems designed using emerging technologies
- Benchmarking of emerging computing technologies from their suitability as a platform for security system design

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 and papers that are in conflict of interest with the guest editors will be rejected. However, such papers can be resubmitted to the regular section.

Guest Editors

- Anupam Chattopadhyay, NTU, Singapore
  (anupam@ntu.edu.sg)
- Swaroop Ghosh, Penn State, USA
  (szg212@engr.psu.edu)
- Debdeep Mukhopadhyay, IIT Kharagpur, India
  (debdeep.mukhopadhyay@gmail.com)
- Wayne Burleson, University of Massachusetts Amherst, USA; AMD
  (burleson@umass.edu)

Important Dates

Manuscript Submission: January 10, 2019

Author Notification: April 20, 2019

Revised Manuscript Submission: May 20, 2019

Final Manuscript Due: July 20, 2019

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 Centre, make sure to do the following:

- Step 1/Type: Make sure to choose "Special Section"
- Step 6/Special Section: Choose "Security for Emerging Technologies" 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/

To avoid delays or automatic rejections, please make sure your manuscript compiles with all TVLSI rules including:

1.Biographies are required for regular papers. Do not submit unless the manuscript has biographies.

2. All authors must be listed in step 3. Make sure the e-mails are up to date, do not create duplicate accounts.

3. If this is not an extension, but there is overlap from your own related publications, a detailed novelty statement needs to be provided after the bio section.

4. A detailed list of differences is needed after the bio section for extensions of previously published work.

5. Upload either a PDF or source file for the manuscript to be reviewed, not both.

6. Manuscripts require IEEE double column format with the figures embedded in the text.

7. To prevent plagiarism, all submissions are scanned with a software that detects overlap with other publications. Papers that have overlap with previous publications (or other sources) and do not include the above novelty statement are automatically rejected and are not allowed to be resubmitted.

A list of frequently asked questions can be found on the ScholarOne Manuscripts homepage when you log into your account.