2nd Workshop on Dependable and Secure Nanocomputing

— Call for Contributions —

Friday June 27, 2008 — Anchorage Hilton Hotel, AK, USA

in conjunction with the 38th Annual IEEE/IFIP International Conference on Dependable Systems and Networks — DSN-2008

Workshop Organizers

Jean Arlat, LAAS-CNRS, Toulouse, France
jean.arlat@laas.fr

Cristian Constantinescu, AMD, Fort Collins, CO, USA
cristian.constantinescu@amd.com

Ravishankar K. Iyer, UIUC, Urbana-Champaign, USA
rkiyer@uiuc.edu

Michael Nicolaïdis, TIMA, Grenoble, France
michael.nicolaidis@imag.fr

Program Committee

Jacob A. Abraham, University of Texas, Austin, USA
Lorena Anghel, TIMA, Grenoble, France
Pradip Bose, IBM T.J. Watson, Yorktown Heights, NY, USA
Jacques Collet, LAAS-CNRS, Toulouse, France
Babak Falsafi, CMU, USA and EPFL, Switzerland
Subhasish Mitra, Stanford University, CA, USA
Shubhendu S. Mukherjee, Intel, Hudson, MA, USA
Takashi Nanya, University of Tokyo, Japan
Rubin A. Parekhji, Texas Instruments, Bangalore, India
Ishwar Parulkar, Sun Microsystems, Santa Clara, CA, USA
Jean-Jacques Quisquater, UCL, Louvain, Belgium
Jaan Raik, Tallinn University of Technology, Estonia
Bruno Rouzeyre, LIRMM, Montpellier, France
Juan Carlos Ruiz García, Univ. Politécnica de Valencia, Spain
Matteo Sonza Reorda, Politecnico di Torino, Italy
Lisa Spainhower, IBM Server Group, Poughkeepsie, NY, USA
Vivian Zhu, Texas Instruments, Dallas, TX, USA
Yervant Zorian, Virage Logic, Fremont, CA, USA

Important Dates

New

- **Papers due:** **March 17, 2008**
- **Acceptance notification:** **April 11, 2008**
- **Final version due:** **May 2, 2008**

Further Information

For more information about DSN-2008 and the venue, please visit the conference web site at: **www.dsn.org**.

Updated information about the workshop can be obtained from **www.laas.fr/WDSN08** or by contacting the workshop organizers.

Motivation and Theme

Unprecedented levels of information processing, novel architectural solutions and a new realm of applications promise to be reached thanks to the advances in semiconductor technologies for integrating extremely large numbers of transistors or processing elements into a chip. Towards this ends, two main tracks are being considered:

- **"More Moore"**: this track is pushing further the long standing Moore's Law-based trend in chip development that aims at reducing the dimensions of silicon microelectronics.
- **"More than Moore"**: this track features atomic assemblies of nanoscale technologies; these include nanowires, carbon nanotubes or organic molecules, etc., and extend also to quantum computing, optical computing and micro/nanofluidics.

Due to the differences in relative advances and current industrial concerns attached to each track, this second edition of the Workshop still plans to emphasize the top-down track for which it is widely recognized such an evolution raises serious challenges both from the Dependability and Security viewpoints. Nevertheless, considerations attached to the above mentioned emerging nanoscale technologies are also part of the scope of the Workshop).

The long standing Moore's Law-based trend in IC development is aiming at nanometric scale elementary devices. Such technologies are already impaired by significant variations affecting process parameters and thus become a nightmare to reliability engineers for reaching an acceptable manufacturing yield at viable cost. The dramatic reduction of digital devices is accompanied by a decrease in power supply and threshold levels which in turn results in lower noise immunity and greater exposure to particles. Moreover, additional instabilities may affect circuit parameters in operation, e.g., negative bias temperature instability (NBTI) in CMOS devices.

Examples of vulnerabilities and malicious threats related to hardware chips are information leakages attached to side channels attacks or differential fault analysis based on applying environmental disturbances or even fault injection. Potential vulnerabilities are also related to the observability and controllability facilities provided by scan-based testing devices.

Scope and Objectives

The Workshop aims at addressing these impairments and threats as well as distinguishing possible alternative design approaches and operation paradigms that are to be enforced and/or favored to keep achieving dependable and secure computing. Three main goals were identified for the Workshop:

- **Review** the state-of-knowledge about main threats in nanocomputing technologies: manufacturing defects, accidental faults, malicious attacks.
- **Identify** existing solutions and **propos**e new solutions attached to various design options for mitigating faults and implementing secure and resilient computing devices and systems.
- **Forecast** the risks associated to emerging technologies and **foster** new trends for cooperative work, possibly combining various alternatives to help increase the pace of advances and solutions.

Topics of Interest, Submission and Information

The workshop is open to all researchers, designers and users involved with or having an interest in dependability and security of hardware technologies. We are interested in submissions from both industry and academia on all topics related to dependable and secure nanocomputing. Potential topics of interest include but are not limited to: emerging nanocomputing paradigms and models, failure modes and risk assessment, yield and mitigation techniques in nanoscale technologies, on-line adaptive and reconfigurable nanoarchitectures, design techniques for developing resilient nanosystems, fault-tolerant architectures specific to nanoscale circuits, scalable verification and testing methodologies, network on chip and communication protocols, etc.

All prospective contributors should submit an extended abstract, work-in-progress report or position paper. Submissions must be original work with no substantial overlap with previously published papers or simultaneous submissions to a journal or conference with proceedings. The submissions should conform to the proceedings publication format (IEEE Conference style) and should not exceed six pages (including all text, references, appendices, and figures). They should explain the contribution to the field and the novelty of the work, making clear the current status of the work. Each submission should start with a title, a short abstract, and names and contact information of the authors. Submissions will be fully refereed by three PC members. Accepted papers will be published in the supplement volume of the DSN 2008 proceedings. Authors of accepted papers must guarantee that their paper will be presented at the Workshop.

Submissions must be made electronically (in PDF format), preferably via the Workshop Webpage (**www.laas.fr/WDSN08**). The organizers can be reached by e-mail at: **dsn2008-nanocomputing[at]laas.fr**.