Guest Editorial
Robust and Energy-Secure Systems

THE "power wall" has forced chip designers and system architects to adopt a variety of techniques to mitigate the power and thermal issues of today's computing systems. Control loops for power and thermal management constitute an example of such kind of facilities, in which a run-time mechanism provisions hardware resources in accordance to the needs of the running workload. In some cases, these features do not perform adjustments in the system, but *just* collect and provide run-time measurements, like in the case of on-chip power and temperature meters. In any case, the ultimate goal of all these new facilities is to enable smaller margins between nominal and worst-case operating points towards "better than worst case" design.

The adoption of such kind of power- and thermal-related capabilities creates all sorts of new challenges for chip and system designers, especially those related to the *robustness* and *security* aspects of the computing system. Examples include stability and robustness of the management control loops, malicious use of the available run-time power and temperature information, potential security vulnerabilities in integrated control loops and management firmware, and system security and safety challenges triggered by violations of energy, reliability, power, or thermal limits. We have coined the term "robust and energy-secure systems" to cover the broad range of research being pursued within industry and academia to ensure reliable and secure operation of systems with integrated power, reliability, and thermal management control loops and metering facilities.

The concept of "robust and energy-secure systems" is already well established in the computer architecture community. For example, members of this Guest Editorial Board have successfully organized three editions of the "Workshop on Energy-Secure System Architectures". Several works in this topic have been already published in premier conferences, forums, and journals [3], [4], [6], [8], [13]. As another example, attackers have compromised crypto keys on smart cards by measuring power consumption patterns arising from repeating crypto operations [9].

In the rest of this editorial, we introduce the papers included in this special issue based on which aspects of robust and energy-secure systems they approach:

- security and robustness of the management control loops;
- system security and safety;
- holistic cross-layer power, reliability, and thermal management solutions.

I. Dynamic Power, Reliability, and Thermal Management: Security and Robustness

The dynamic provisioning and management of hardware resources constitutes one of the most promising (and widely adopted) strategies to deal with system power and thermal issues. In particular, *dynamic voltage and frequency scaling* (DVFS) [10], [12] and *clock gating* [2], [10] constitute two of the most popular "knobs." DVFS provides an effective mechanism for power and thermal management, by enabling the system to adjust voltage and frequency dynamically. Clock gating aims at reducing dynamic power consumption by disabling parts of the clock distributions networks. In this special issue, two papers address the security and robustness aspects of dynamic voltage scaling and clock gating. In "Converter-Gating: A Power Efficient and Secure on-Chip Power Delivery System," Uzun *et al.* present a workload aware, *secure* regulator-gating technique, in which switched capacitor (SC) voltage converters are adaptively turned *on* and *off* based on the workload characteristics to improve voltage conversion efficiency. Equally important, the turn on and off pattern of the SC voltage converters is randomized to scramble the power consumption profile as a countermeasure to power analysis-like side-channel attacks. In "BTI-Gater: An Aging-Resilient Clock Gating Methodology," Lai *et al.* present a technique to minimize the effects of negative- and positive bias temperature instability (N/PBTI) on clock distribution networks with clock gating features. The authors propose a new approach to design integrated clock gating (ICG) cells, named "BTI-Gater cells," which aims at balancing the amount of time that the clock distribution network stays in logic high and logic low states during clock gating periods. The authors also recognize potential vulnerabilities associated with BTI-Gater, namely a case where the running application exhibits a phase that always results in very short clock gating periods and another phase that always results in very long clock gating periods. The authors propose a simple yet effective software-level mitigation technique to tackle this issue.

II. System Security and Safety

Differential power analysis (DPA) [7] is a well-known side channel attack, which consists in statistically analyzing power consumption measurements to obtain secret information from a computing system (like, for example, cryptographic keys). The proliferation of all sorts of on-chip power and temperature meters in today's computing systems turns DPA into a dangerously attractive security exploit. In this special issue, two papers address the DPA problem and present novel strategies to alleviate it. In "A Performance and Area Efficient ASIP for Higher-Order DPA-Resistant AES," Wang *et al.* address the crucial problem of implementing efficient countermeasures against side-channel DPA attacks. A well studied countermeasure based on masking is considered and efficient implementations of the Advanced Encryption Standard (AES) are presented by extending the instruction set architecture. The

Digital Object Identifier 10.1109/JETCAS.2014.2315885

expensive AES operations of *SubBytes* and *MixColumns* are implemented in hardware, while the remaining AES operations are performed in software. In "A Methodology for Optimized Design of Secure Differential Logic Gates for DPA Resistant Circuits," Tena-Sánchez *et al.* present a design methodology to improve the tolerance of logic gates against DPA attacks with low performance impact. The proposed approach is based on a dual rail with precharge logic (DPL), specifically sense amplifier based logic (SABL).

III. Robustness and Energy-Security Across the Hardware/Software Stack

Holistic (hardware-software stack) power, reliability, and thermal management solutions became popular since the advent of cross-layer standards for system device configuration, like the advanced configuration and power interface (ACPI) [1], [11]. The goal is to benefit from the characteristics of the different "layers" in the stack to improve the management of system resources. For example, circuit-level techniques (like DVFS and clock gating) provide fast actuation and can be very effective for fine resource provisioning; however, they inherently have a limited operation scope (e.g., the core, processor, or memory). On the other hand, software-level techniques (like processor folding [5] and hardware virtualization) benefit from a comprehensive view of the system "which can lead to better longer-term management decisions," but at the expense of more significant operation overheads. In this special issue, two papers approach the power and reliability management issue with hardware/software stack solutions. In "Improving Resilience to Timing Errors by Exposing Variability Effects to Software in Tightly-Coupled Processor Clusters," Rahimi *et al.* propose a *process variation*-aware scheduling approach for chip multiprocessors, based on OpenMP extensions. These extensions operate at software level, with support of hardware-provided profiling information. The scheduler makes use of this profiling information to determine the vulnerability of the different software constructions and allocates tasks across cores to improve energy efficiency. In this regard, this work constitutes a good example of a holistic, cross-layer solution. In "A Custom MPSoC Architecture with Integrated Power Management for Real-Time Neural Signal Decoding," Carta *et al.* address a very critical problem in today's *ubiquitous computing* domain, namely how to meet the real-time constraints of critical neuro-controlled motor prostheses applications while still providing power efficiency. The authors present a proof-of-concept of a power-aware chip multiprocessor (CMP) for real-time neural signal decoding, as well as an efficiency-aware approach for the parallelization of (usually sequential) neural signal processing algorithms. This work encompasses hardware-level (the CMP architecture) and software-level (the efficiency-aware parallel algorithm) solutions and, hence, constitutes another good cross-layer approach example.

IV. Selection Process of the Special Issue

The review and selection process consisted of two rounds. During the first round, we assigned expert reviewers to each submission and the selected ones were asked to be revised. We conducted a second round of reviews on the revised submissions to satisfy the high-quality requirements of the IEEE Journal on Emerging and Selected Topics in Circuits and Systems.

Finally, we would like to thank all the authors who submitted their papers to this special issue, either if they were accepted or not. We also express our deep gratitude to all the reviewers for their valuable time and volunteering efforts which helped the authors to considerably improve the technical quality of the accepted papers. A special thanks to the members of our Supporting Committee, who did a great job of publicizing the special issue: Pradip Bose (IBM Research, USA), Alper Buyuktosunoglu (IBM Research, USA), Ramón Canal (UPC Barcelona, Spain), Dimitris Gizopoulos (University of Athens, Greece), Hiroshi Nakamura (University of Tokyo, Japan), and Hiroshi Sasaki (Kyushu University, Japan).

We sincerely hope that you enjoy this special issue and find its contents informative and useful!

Augusto Vega, *Guest Editor*
IBM T. J. Watson Research Center
IBM Corporation
Yorktown Heights, NY 10598 USA

Simha Sethumadhavan, *Guest Editor*
Department of Computer Science
Columbia University
New York, NY 10027 USA

Subhasish Mitra, *Guest Editor*
Department of Electrical Engineering
Stanford University
Stanford, CA 94305 USA

References

[1] ACPI, ACPI overview [Online]. Available: http://www.acpi.info/presentations/ACPI_Overview.pdf 2004

[2] L. Benini, P. Siegel, and G. De Micheli, "Automatic synthesis of gated clocks for power reduction in sequential circuits," *IEEE Design Test Comput.*, pp. 32–40, 1994.

[3] P. Bose, "Energy-secure computing," in *Proc. 2012 ACM/IEEE Int. Symp. Low Power Electron. Design.*, 2012, pp. 1–2.

[4] P. Bose, A. Buyuktosunoglu, J. Darringer, M. Gupta, M. Healy, H. Jacobson, I. Nair, J. Rivers, J. Shin, A. Vega, and A. Weger, "Power management of multi-core chips: Challenges and pitfalls," in *Proc. Design, Automat. Test Eur. Conf.*, 2012, pp. 977–982.

[5] M. Broyles, C. Francois, A. Geissler, M. Hollinger, T. Rosedahl, G. Silva, J. V. Heuklon, and B. Veale, IBM EnergyScale for POWER7 Processor Based Systems [Online]. Available: ftp://public.dhe.ibm.com/common/ssi/ecm/en/pow03039usen/POW03039USEN.PDF 2013

[6] J. Demme, R. Martin, A. Waksman, and S. Sethumadhavan, "A quantitative, experimental approach to measuring processor side-channel security," *IEEE Micro*, vol. 33, no. 3, pp. 68–77, May 2013.

[7] P. C. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proc. 19th Annu. Int. Cryptol. Conf. Adv. Cryptol.*, 1999, pp. 388–397.

[8] A. Lungu, P. Bose, A. Buyuktosunoglu, and D. J. Sorin, "Dynamic power gating with quality guarantees," in *Proc. 14th ACM/IEEE Int. Symp. Low Power Electron. Design*, 2009, pp. 377–382.

[9] S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks: Revealing the Secrets of Smart Cards (Advances in Information Security)*. New York: Springer-Verlag, 2007.

[10] P. R. Panda, A. Shrivastava, B. Silpa, and K. Gummidipudi, *Power-Efficient System Design*, 1st ed. New York: Springer, 2010.

[11] B. Steigerwald, C. Lucero, C. Akella, and A. Agrawal, *Energy Aware Computing: Powerful Approaches for Green System Design*, 1st ed. Santa Clara, CA: Intel Press, 2011.

[12] A. Vassighi and M. Sachdev, *Thermal and Power Management of Integrated Circuits*, 1st ed. New York: Springer, 2006.

[13] Z. Wu, M. Xie, and H. Wang, "On energy security of server systems," *IEEE Trans. Depend. Secure Comput.*, vol. 9, no. 6, pp. 865–876, Nov. 2012.

Augusto Vega was born in Realicó, Argentina, in 1979. He received the M.Sc. degree in computer architecture, networks and systems, and the Ph.D. degree in computer architecture from Polytechnic University Catalonia, Barcelona, Spain, in 2009 and 2013, respectively.

He is a Research Staff Member within the Reliability and Power-Aware Microarchitecture Department at IBM T. J. Watson Research Center. He has been involved in research and development work in support of IBM System p and Data Centric Systems. His primary focus area is power-aware computer architectures and associated system solutions. He has developed techniques to reduce chip power consumption in multicore/manycore chips for multi-threaded applications, exploiting core folding, frequency/voltage scaling, and low-power ("sleep") modes. He has several pending/issued patents, mostly in the area of power-aware computer architectures. His research interests include high performance, power/reliability-aware computer architectures, distributed and parallel computing, and performance analysis tools and techniques.

Dr. Vega has served as a reviewer for many journals and international conferences. He currently serves as a Guest Editor for the IEEE Micro Special Series on "Harsh Chips." He is also actively involved in the organization of several workshops and tutorials ("HARSH: Workshop on Highly-Reliable Power-Efficient Embedded Designs," "ESSA: Workshop on Energy-Secure System Architectures," "FastPath: Workshop on Performance Analysis of Workload Optimized Systems").

Simha Sethumadhavan (M'10) received the Ph.D. degree from the University of Texas at Austin, Austin, TX, USA, in 2007.

He is an Associate Professor of Computer Science at Columbia University. His research interests are in hardware security and energy-efficient computing. He is the principal investigator on the DARPA SPARCHS project at Columbia University. The goal of the project is to discover how systems should be designed if security was a first-order design requirement in addition to the traditional requirements like power/performance, etc.

Dr. Sethumadhavan has been recognized with an Alfred P Sloan Fellowship (2013), NSF CAREER award (2011), two IEEE Micro "top pick" awards (2004, 2013), and a graduate teaching award (2006).

Subhasish Mitra (F'13) directs the Robust Systems Group in the Department of Electrical Engineering and the Department of Computer Science of Stanford University, where he is the Chambers Faculty Scholar of Engineering Before joining Stanford, he was a Principal Engineer at Intel Corporation. His research interests include robust system design, VLSI design, CAD, validation and test, and emerging nanotechnologies. His X-Compact technique for test compression has been key to cost-effective manufacturing and high-quality testing of a vast majority of electronic systems, including numerous Intel products. X-Compact and its derivatives have been implemented in widely-used commercial electronic design automation tools. The QED and IFRA techniques, created jointly with his students, have shown outstanding results in overcoming critical bottlenecks in post-silicon validation and debug for several commercial hardware platforms, and have been characterized as "breakthrough" in a Research Highlight in the *Communications of the ACM*. His work on carbon nanotube imperfection-immune digital VLSI, jointly with his students and collaborators, resulted in the demonstration of the first carbon nanotube computer, and it was featured on the cover of *Nature*. The National Science Foundation (NSF) presented this work as a Research Highlight to the United States Congress, and it also was highlighted as "an important, scientific breakthrough" by the BBC, Economist, EE Times, IEEE Spectrum, MIT Technology Review, National Public Radio, New York Times, Scientific American, Time, Wall Street Journal, Washington Post, and numerous other organizations worldwide.

Prof. Mitra’s honors include the Presidential Early Career Award for Scientists and Engineers from the White House, the highest United States honor for early-career outstanding scientists and engineers, IEEE CAS/CEDA Pederson Award, and the Intel Achievement Award, Intels highest corporate honor. He and his students published several award-winning papers at major venues: IEEE/ACM Design Automation Conference, IEEE International Solid-State Circuits Conference, IEEE International Test Conference, IEEE Transactions on CAD, IEEE VLSI Test Symposium, Intel Design and Test Technology Conference, and the Symposium on VLSI Technology. At Stanford, he was honored several times by graduating seniors “for being important to them during their time at Stanford.” He has served on numerous conference committees and journal editorial boards. Recently, he served on Defense Advanced Research Projects Agencys Information Science and Technology (ISAT) Board as an invited member.