# Preface

## Ed F. Deprettere

Leiden Embedded Research Center,
Leiden Institute of Advanced Computer Science,
Leiden University, 2333 CA Leiden, The Netherlands
E-mail: edd@liacs.nl

## Shuvra S. Bhattacharyya

Department of Electrical and Computer Engineering, and
Institute for Advanced Computer Studies,
University of Maryland, College Park, MD, USA
E-mail: ssb@umd.edu

**Biographical notes:** Ed F. Deprettere is fellow of the IEEE. He received the MSc Degree from the University of Ghent, Ghent, Belgium, in 1968, and the PhD Degree from the Delft University of Technology, Delft, The Netherlands, in 1981. From 1980–1999 he was Professor at the Department of Electrical Engineering, Circuits and Systems section, Signal Processing Group. From 1st January 2000, he is Professor at the Leiden Institute of Advances Computer Sciences, Leiden University, Leiden, The Netherlands, where he is Head of the Leiden Embedded Research Center. His current research interests are in system level design of embedded systems, in particular for signal, image and video processing applications, including wireless communications and multimedia. He is editor and co-editor of four books and several special issues of international journals. He is on the editorial board of three journals.

Shuvra S. Bhattacharyya is a Professor in the Department of Electrical and Computer Engineering and the Institute for Advanced Computer Studies (UMIACS) at the University of Maryland, College Park. His research interests include VLSI signal processing; biomedical circuits and systems; embedded software; and hardware/software co-design. He received the BS Degree from the University of Wisconsin at Madison, and the PhD Degree from the University of California at Berkeley. He has held industrial positions as a researcher at the Hitachi America Semiconductor Research Laboratory (San Jose, California), and as a Compiler Developer at Kuck & Associates (Champaign, Illinois).

The current issue and previous issue of the *International Journal on Embedded Systems* are organised as companion special issues that are based on the theme of *Systems and Architectures for Embedded Processing*. These two issues contain a selection of top papers from the *2003 International Conference on Application-specific Systems, Architectures, and Processors (ASAP 2003)* and the *2003 International Workshop on Systems, Architectures, Modeling, and Simulation (SAMOS 2003)*. *ASAP* and *SAMOS* (now the *International Conference on Embedded Computer Systems: Architectures, Modeling, and Simulation*) are two annual forums that focus on technology for design and implementation of embedded systems. *ASAP 2003* was located in The Hague, The Netherlands under the organisation of Ed Deprettere and Shuvra Bhattacharyya (General Co-Chairs), and Lothar Thiele, Alain Darte, and Joseph Cavallaro (Program Co-Chairs). *SAMOS 2003* was located, as all meetings of this forum have been held, in Samos, Greece. *SAMOS 2003* was organised by Stamatis Vassiliadis.

Our two companion issues are organised under the subthemes of *Applications and Hardware* (this issue), which covers selected papers from *ASAP 2003*, and *Design Methods and Tools* (the previous issue), which covers selected papers from *SAMOS 2003* and additional selected papers from *ASAP 2003*.

Two papers in this special issue involve hardware design considerations for efficient communication networks in multiprocessor systems. In 'Application-specific permutation networks', Dräeger and Fettweis develop grouptheoretic methods to derive specialised interconnection networks in a systematic manner. A variety of heuristics are integrated into the approach to improve the scalability of the techniques.

In 'On-chip implementation of multiprocessor networks and switch fabrics', Ye and De Micheli describe a network floorplanning tool for multiprocessor system-on-chip implementation. The tool is specifically geared towards architectures involving homogeneous processors and regular connection topologies, and it preserves this regularity in the derived solutions while providing significant reductions in wire length requirements.

Three papers develop novel techniques for acceleration of cryptographic applications. In 'Alternative application-

specific processor architectures for fast arbitrary bit permutations', Shi et al. motivate bit permutation being the critical operation for efficient implementation block ciphers. The paper presents and compares several different application-specific instruction-set processor approaches that achieve arbitrary 64-bit permutations within two cycles without any degradation in cycle time compared to typical arithmetic logic units.

In 'Hardware implementation of an elliptic curve processor over $GF(p)$ with Montgomery modular multiplier', Örs et al. present an efficient arithmetic processor for elliptic curve cryptography. An FPGA implementation is reported that requires less memory and provides higher performance compared to previous approaches.

In 'A cryptographic processor for arbitrary elliptic curves over $GF(2^m)$', Eberle et al. present a flexible processor for elliptic curve cryptography. The processor gives optimised performance for selected named curves while also handling generic curves over arbitrary fields, and this heterogeneity is supported without any need for reconfiguration.

Three papers develop optimisation techniques that are geared towards design of signal processing systems. In 'Code compression in DSP processor systems', Saastamoinen et al. develop a number of alternative compression techniques for reducing on-chip memory requirements on programmable digital signal processors. Their experimental evaluation shows that the best technique provides 40% and 45% reductions in area requirements for audio and video applications, respectively, when taking into account the area overhead for decompression.

In 'An efficient disk-array-based server design for multicast video streaming system', Chan and Lee present methods for placement and retrieval of video that support both periodic and aperiodic streaming channels. The paper also proposes a zoning technique that can be integrated with the video placement method to improve disk utilisation.

In 'Hardware synthesis for systems of recurrence equations with multi dimensional schedule', Guillou et al. develop a systematic approach for mapping recurrence equations into hardware based on multidimensional schedules. The techniques are demonstrated on a matrix multiplication example that is synthesised into VHDL code based on the proposed methods.

The remaining two papers address hardware implementation issues that are relevant to energy consumption and safety enhancement, respectively, of application-specific architectures. In 'A hardware mechanism to reduce the energy consumption of the register file of in-order architectures', Ayala et al. develop an approach for saving energy in embedded processors by placing unused registers into low power states, and activating the registers when they are needed by active instructions. The method is shown to provide large reductions in power consumption without any loss in performance.

In 'Safe execution of untrusted applications on embedded network processors', Bos et al. propose a framework for allowing applications to exploit the low level capabilities of a shared network processor without compromising the safety of the overall system. The framework is designed for scenarios in which the overhead of providing safety is more than offset by the performance gain achieved through better use of the network processor.

We would like to thank Laurence Yang for his support of this special issue. We would also like to thank the organisers and program committee members of *ASAP 2003*, and the authors of the informative papers that appear in this issue.