Journal of VLSI Signal Processing 47, 1–2, 2007

DOI: 10.1007/s11265-006-0035-4

Editorial for the Special Issue on Field Programmable Technology

This special issue on Field Programmable Technology contains extended versions of six papers that were presented at the Fourth IEEE International Conference on Field Programmable Technology (FPT '05). This conference has a vital role in providing an Asia-Pacific forum for bringing together FPT researchers from around the globe. The fourth conference was hosted by the National University of Singapore on 11–14 December 2005. There were two invited keynote talks, 32 full paper presentations and 30 poster presentations. The program emphasized field-programmable devices and architectures, configurable architectures and reconfigurability, design methodologies and tools, and novel applications of field-programmable technology.

The six papers selected for this special issue were amongst those papers most highly ranked by the distinguished international panel of reviewers for the conference. The authors were invited to prepare extended versions of their conference papers that would be appropriate for journal publication. We thank the authors for doing this, and to the international reviewers who assisted in providing insightful feedback on these submissions, leading to the final versions of the papers that are published here.

The range of the papers provides a flavor of the state of the art in Field Programable Technology today, with a particular emphasis on novel applications. We feel that a focus on high-quality real-life application of this technology will be of particular interest to the readership of the journal. After all, without realistic applications, research effort on devices, architectures, and design methodologies, becomes harder to justify—in the medium term at least. Thus four of the six papers included here have a primary focus on applications, and indeed illustrate a diverse collection of applications.

The first paper, "The Architecture and Development Flow of the S5 Software Configurable Processor" by Arnold, presents a new software configurable processor. This is a hybrid device that couples a conventional processor datapath with programmable logic to allow application programs to dynamically customize the instruction set. Performance gains of more than an order of magnitude over a processor without the added acceleration capability are reported. The paper gives a convincing illustration of how the traditionally separate worlds of processors and programmable logic can be integrated in order to deliver a true field programmable technology.

The second paper, "The Erlangen Slot Machine: A Dynamically Reconfigurable FPGA-Based Computer" by Majer et al, shows a different technical direction, where programmable logic is harnessed in order to build a complete computing machine. This is a new highly flexible platform in which each functional component need not be fixed permanently at a given location in the programmable logic array, allowing dynamic reconfiguration of system modules at run time. Furthermore, the paper also describes a flexible mechanism for communication between modules, a subject often neglected in earlier proposals of this type, and something crucial for effective application support.

The third paper, "Designing a Posture Analysis System with Hardware Implementation" by Coutinho et al, is the first of the four applications papers. It concerns posture analysis, an active research area in computer vision, here with a particular aim of building a pervasive visual sensing environment that can monitor and assess daily activities of home care patients. One of the designs reported, which targets a single programmable logic device, shows a 145-fold speedup over a software version running on a processor. The video frame rate is well above that required for real-time video, allowing the sharing of the system amongst multiple video sources.

The fourth paper, "High Speed and Low Area Hardware Architectures of the Whirlpool Hash Function" by McLoone and McIvor, presents a

high-speed hardware architecture for the Whirlpool hash function, which is a collision-resistant 512-bit hash function used as part of signature and integrity security protocols. Several designs targeted at programmable logic are reported, with an unrolled version of the architecture achieving a throughput of 4.9 Gbps, which is faster than earlier implementations of this algorithm and of other hashing algorithms, such as SHA-512. The paper gives an insight into the raw computational power available in field programmable technologies.

The fifth paper, "A Custom Instruction Approach for Hardware and Software Implementations of Finite Field Arithmetic over F_(2^163) using Gaussian Normal Bases" by Juliato et al, is also drawn from the security domain. As in the first paper, the approach is to add custom instructions to an existing processor, the benefit coming from acceleration of the finite-field arithmetic operations that are fundamental to elliptic curve cryptography (ECC), an appealing approach for public-key cryptography. The paper reports that, by accelerating finite field multiplication using field programmable technology, point multiplication for ECC can be accelerated over 116-fold.

Finally, the sixth paper, "High Quality Uniform Random Number Generation using LUT Optimised State-Transition Matrices" by Thomas and Luk, describes a class of efficient uniform random number generators that is optimized for the characteristics of contemporary programmable logic arrays. These generators have applications in Monte Carlo integration, simulated annealing, and financial simulations. One of the reported examples is a 32-bit random number generator with a period of 2^{160} that passes all common empirical randomness tests, and is capable of operating at rates in excess of 10 Gbps, while using very small programmable logic resource.

In summary, we hope that, from this small selection of papers, readers will appreciate the flavor of some current research in the general area of field programmable technologies, and in particular get a feeling for the inherent computational power that is available from such technologies. For the future, a key research challenge is devising the computational abstractions, and then the appropriate associated design tools, that allow the raw power of the technology to be made available in a form that facilitates easy mapping of particular applications.

Guest Editors

Gordon Brebner
Xilinx, Inc., USA
gordon.brebner@xilinx.com

Samarjit Chakraborty

Weng-Fai Wong
National University of Singapore, Singapore