Welcome to ASAP 2008: the 19th IEEE International Conference on Application-specific Systems, Architectures and Processors. This year’s event takes place in the historic university town of Leuven, Belgium. The history of the event traces back to the International Workshop on Systolic Arrays, organized in 1986 in Oxford, UK. It later developed into the International Conference on Application Specific Array Processors. With its current title, it was organized for the first time in Chicago, USA in 1996. Since then it has alternated between Europe and North-America.

The ASAP conferences provide a forum for researchers and practitioners from academia and industry interested in both the fundamental principles of application-specific computing systems and architectures, as well as their practical adoption in a wide variety of application domains. Results presented at these conferences have had a significant impact on systems architecture, reconfigurable computing, design automation, automatic parallelization, and on application domains such as embedded systems, computer arithmetic, signal and image processing, cryptographic hardware and systems.

After more than 20 years, ASAP is still a thriving conference. In response to the call for papers, 113 submissions were received. These submitted papers came from 25 countries in Asia, Europe, North America, and South America. A rigorous review process resulted in 36 papers for lecture presentations and 17 papers for interactive presentation at the conference. These are complemented by keynote talks by Ruby Lee (Princeton University) and Gert Goossens (Target Compiler Technologies).
The session titles summarize the variety of the topics covered:

- Application-Specific Processor Instruction-Sets
- System-Level Interconnect and Mapping in SoCs
- Advances in Cryptography
- New Computational Methods
- Novel Applications
- New Directions
- Acceleration of Scientific and DSP Applications
- Advanced Communications Applications
- Arithmetic
- Interconnect and Mapping
- Novel Processor and Memory System Techniques
- Image and Video Processing

We thank the keynote speakers and all the authors who responded to the call for papers. We also thank members of the Program Committee and the External Referees who generously offered their expertise and completed the reviews on time. We are grateful to our primary sponsors – the IEEE Computer Society and IMEC. We particularly thank the great efforts of Murali Jayapala, Andy Lambrechts, Fred Loosen, Praveen Raghavan, Annemie Stas, Myriam Janowski, Daniella Van Ravesteijn and Marcel Gort. The conference would not have run so smoothly without the selfless contributions of these individuals.

We are proud of history of ASAP, which has provided opportunities for collaboration, the development of new talents, and a platform for dissemination of new ideas. We look forward to your participation in ASAP 2008 and in future years.

Ingrid Verbauwhede, Diederik Verkest and Steve Wilton
IEEE
19th International Conference on

**Application-Specific Systems, Architectures and Processors**

Leuven, Belgium, July 2 - 4, 2008

**TABLE OF CONTENTS**

ASAP Organizing and Steering Committees .......................................................... viii
ASAP Technical Program Committee ................................................................. ix
Keynote 1: Security and Ubiquity Opportunities for Application-Specific Processors, Ruby B. Lee ................................................................. xi
Keynote 2: The Art of Application-Specific Processor Design: Great Artists use Good Tools, Gert Goossens ................................................................. xiii
Session 1: Application-Specific Processor Instruction Sets .................................... 1
- Fast Custom Instruction Identification by Convex Subgraph Enumeration .......... 1
- Bit Matrix Multiplication in Commodity Processors ........................................ 7

Interactive Session 1 ......................................................................................... 13
- Synthesis of Application Accelerators on Runtime Reconfigurable Hardware .... 13
- Floating Point Multiplication Rounding Schemes for Interval Arithmetic .......... 19
- Fast Multivariate Signature Generation in Hardware: The Case of Rainbow .... 25
- Fault-Tolerant Dynamically Reconfigurable NoC-based SoC ......................... 31
- Security Processor with Quantum Key Distribution ....................................... 37
- Fully-Pipelined Efficient Architectures for FPGA Realization of Discrete Hadamard Transform ................................................................. 43
- Reconfigurable Viterbi Decoder on Mesh Connected Multiprocessor Architecture ..... 49
- Run-time Thread Sorting to Expose Data-level Parallelism ............................ 55

---

IEEE Catalog number: CFP08083
Library of Congress: 2007908829

© 2008 IEEE. Personal use of this material is permitted. However, permission to reprint/republish this material for advertising or promotional purposes or for creating new collective works for resale or redistribution to servers or lists, or to reuse any copyrighted component of this work in other works must be obtained from the IEEE.
Session 2: System-level Interconnect and Mapping in SoCs ......................... 61
- A New High-Performance Scalable Dynamic Interconnection for FPGA-based Reconfigurable Systems ................................................................. 61
- Extending the SIMPPL SoC Architectural Framework to Support Application-Specific Architectures on Multi-FPGA Platforms ............................ 67
- PERMAP: A Performance-Aware Mapping for Application-Specific SoCs .... 73

Session 3: Advances in Cryptography .......................................................... 79
- Low-cost Implementations of NTRU for Pervasive Security ...................... 79
- On the High-Throughput Implementation of RIPEMD-160 Hash Algorithm .... 85
- Zodiac: System Architecture Implementation for a High-Performance Network Security Processor ................................................................. 91

Session 4: New Computational Methods ....................................................... 97
- Efficient Systolization of Cyclic Convolution for Systolic Implementation of Sinusoidal Transforms ................................................................. 97
- Resource Efficient Generators for the Floating-point Uniform and Exponential Distributions ................................................................. 102
- Low Discrepancy Sequences for Monte Carlo Simulations on Reconfigurable Platforms ................................................................. 108

Session 5: Novel Applications .................................................................... 114
- A Subsampling Pulsed UWB Demodulator Based on a Flexible Complex SVD .... 114
- Dynamically Reconfigurable Regular Expression Matching Architecture ........ 120
- An MPSoC Architecture for the Multiple Target Tracking Application in Driver Assistant System ................................................................. 126

Session 6: New Directions in Application-Specific Design ......................... 132
- Managing Multi-Core Soft-Error Reliability Through Utility-driven Cross Domain Optimization ................................................................. 132

Interactive Session 2 ............................................................................. 138
- An Efficient Implementation Of A Phase Unwrapping Kernel On Reconfigurable Hardware ................................................................. 138
- A Parallel Hardware Architecture for Connected Component Labeling Based on Fast Label Merging ................................................................. 144
- Operation Shuffling over Cycle Boundaries for Low Energy L0 Clustering .... 150
- An Efficient Digital Circuit for Implementing Sequence Alignment Algorithm in an Extended Processor ................................................................. 156
- Concurrent Systolic Architecture for High-Throughput Implementation of 3-Dimensional DWT ................................................................. 162
- Hierarchical Design Space Exploration of a Cooperative MIMO Receiver for Reconfigurable Architectures ................................................................. 167
- A Dynamic Holographic Reconfiguration on a Four-Context ODRGA .......... 173
· FGPA-based Hardware Accelerator of the Heat Equation with Applications on Infrared Thermography ................................................................. 179
· FPGA Based Singular Value Decomposition for Image Processing Applications...... 185

Session 7: Acceleration of Scientific and DSP Applications .................. 191
· Accelerating Nussinov RNA secondary structure prediction with systolic arrays on FPGAs.............................................................................. 191
· A Multi-FPGA Application-Specific Architecture for Accelerating a Floating Point Fourier Integral Operator ......................................................... 197
· Reconfigurable Acceleration of Microphone Array Algorithms for Speech Enhancement ...................................................................................... 203

Session 8: Advanced Communications Applications ..................... 209
· Configurable and Scalable High Throughput Turbo Decoder Architecture for Multiple 4G Wireless Standards ......................................................... 209
· Architecture and VLSI Realization of a High-Speed Programmable Decoder for LDPC Convolutional Codes .......................................................... 215
· Buffer allocation for Advanced Packet Segmentation in Network Processors.... 221

Session 9: Arithmetic................................................................. 227
· New Insights on Ling Adders ........................................................................ 227
· Integer and Floating-Point Constant Multipliers for FPGAs ...................................... 233
· An Efficient Method for Evaluating Polynomial and Rational Function Approximations ........................................................................................... 239

Session 10: Interconnect and Mapping ........................................ 245
· Mapping of the AES Cryptographic Algorithm on a Coarse-Grain Reconfigurable Array Processor ........................................................................ 245
· RECONNECT: A NoC for polymorphic ASICs using a Low Overhead Single Cycle Router ......................................................................................... 251
· Loop-Oriented Metrics for Exploring and Application-Specific Architecture Design-Space ...................................................................................... 257

Session 11: Novel Processor and Memory System Techniques .......... 263
· Rapid Estimation of Instruction Cache Hit Rates Using Loop Profiling ............ 263
· Reducing Power Consumption of Embedded Processors through Register File Partitioning and Compiler Support .............................................. 269
· Lightweight DMA Management Mechanisms for Multiprocessors on FPGA...... 275
· Memory Copies in Multi-Level Memory Systems ........................................ 281

Session 12: Image and Video Processing ..................................... 287
· Architecture of a Polymorphic ASIC for interoperability across multi-mode H.264 decoders ................................................................. 287
· An FPGA Architecture for CABAC Decoding in Many-core Systems ........ 293
· Novel Approach on Lifting-Based DWT and IDWT Processor with Multi-Context Configuration to Support Different Wavelet Filters ......................................................... 299
· Throughput-Scalable Hybrid-Pipeline Architecture for Multilevel Lifting 2-D DWT of JPEG 2000 Coder ........................................................................................................ 305

Author Index .............................................................................................................................................................................. 310
ASAP ‘08 Organizing Committee

General Chair
Diederik Verkest, IMEC, Belgium

Technical Program Chairs
Ingrid Verbauwhede, K.U.Leuven, Belgium
Steve Wilton, University of British Columbia, Canada

Publication Chair
Andy Lambrechts, IMEC, Belgium

Web Management Chair
Praveen Raghavan, IMEC, Belgium

Publicity Chair
Murali Jayapala, IMEC, Belgium

Local Arrangements
Annemie Stas, IMEC, Belgium
Fred Loosen, IMEC, Belgium

ASAP Steering Committee

Jose Fortes, University of Florida
S-Y Kung, Princeton University
Wayne Luk, Imperial College
Michael Schulte, University of Wisconsin
Earl Swartzlander, University of Texas
ASAP Technical Program Committee

El Mostapha Aboulhamid, U. de Montréal
Amirali Baniasadi, U. of Victoria
Jürgen Becker, U. Karlsruhe
Koen Bertels, Delft U. of Technology
Shuvra Bhattacharyya, U. of Maryland
Gordon Brebner, Xilinx Inc.
Geoffrey Brown, India U.
Peter Cappello, U. of California at Santa Barbara
Joseph Cavallaro, Rice U.
Chaitali Chakrabarti, Arizona State U.
Karam Chatha, Arizona State U.
Liang-Gee Chen, National Taiwan U.
George Constantinides, Imperial College
Jean-Pierre David, École Polytechnique de Montréal
Gerhard Fettweis, Dresden U. of Technology
Georgi N. Gaydadjiev, Delft U. of Technology
Peter Hallschmid, U. of British Columbia
Paolo Ienne, École Polytechnique Fédérale de Lausanne
Tom Kean, Algotronix
Israel Koren, U. of Massachusetts at Amherst
Georgi Kuzmanov, Delft U. of Technology
Pierre Langlois, École Polytechnique de Montréal
Ruby B Lee, Princeton U.
Miriam Leeser, Northeastern U.
Philip Leong, Chinese U. of Hong Kong
Dake Liu, Linköping University
Wayne Luk, Imperial College
Liam Marnane, U. College Cork
Grant Martin, Tensilica
Oskar Mencer, Imperial College
Heinrich Meyr, Rheinisch-Westfälische Technische Hochschule Aachen
Tulika Mitra, National U. of Singapore
Jean-Michel Muller, ÉNS de Lyon
Alex Nicolau, U. of California, Irvine
Gabriela Nicolescu, École Polytechnique de Montréal
Tobias Noll, Rheinisch-Westfälische Technische Hochschule Aachen
Jari Nurmi, Tampere University of Technology
Peter Pirsch, U. of Hannover
Gang Qu, U. of Maryland
Patrice Quinton, IRISA
Sanjay Rajopadhye, Colorado State U.
Daler Rakhmatov, U. of Victoria
Tanguy Risset, ÉNS de Lyon
Frédéric Rousseau, TIMA
Kentar Sano, Tohoku U.
Yvon Savaria, École Polytechnique de Montréal
Lesley Shannon, Simon Fraser University
Dirk Stroobandt, Ghent University
Henry Styles, Xilinx Inc.
Juergen Teich, Erlangen U.
Alexander Tenca, Synopsys Inc.
Lothar Thiele, ETH
Tom Vander Aa, IMEC
Ingrid Verbauwhede, K.U.Leuven
Doran Wilde, Brigham Young U.
Steve Wilton, U. of British Columbia
Roger Woods, Queen's U. of Belfast
Pen-Chung Yew, U. of Minnesota at Twin Cities
Cedric Yiu, Hong Kong Polytechnic University
Clifford Young, D. E. Shaw group
Keynote 1:
Security and Ubiquity Opportunities for Application-Specific Processors, Ruby B. Lee

Abstract

Application-specific processors have been designed for improving the performance of a given important application or class of applications. They have also enabled improvements in power consumption, cost, size and efficiency. With the escalating number of attacks on computing, communications and entertainment devices, the issue of security is now of paramount importance. How can application-specific instruction processors (ASIPs) be designed to significantly improve applications security? Can the hardware provide fundamental security enablers for an application, beyond cryptographic acceleration? At the same time, is there a way to make ASIPs more ubiquitous? Can insights gained from application-driven design be generalized? This talk will discuss some of the opportunities for application-specific processor architectures to innovate and lead the way in building security features into processors. It will also discuss how ASIP designs can be “generalized”, leading to more ubiquitous deployment of novel and efficient processing techniques gleaned from application-driven designs.

Speaker’s Bio

Ruby B. Lee is the Forrest G. Hamrick Professor of Engineering and Professor of Electrical Engineering at Princeton University, with an affiliated appointment in the Computer Science Department. She is the director of the Princeton Architecture Laboratory for Multimedia and Security (PALMS). Her current research is in designing security-aware processors, memories and systems, protecting critical information, and designing innovative instruction-set architecture for emerging computing paradigms. She is a Fellow of the ACM, Fellow of the IEEE and Associate Editor-in-Chief of IEEE Micro.

Prior to joining the Princeton faculty in 1998, Dr. Lee served as chief architect at Hewlett-Packard, responsible at different times for processor architecture, multimedia architecture and security architecture. She was a key architect of the PA-RISC architecture used for HP workstations and servers. She pioneered adding multimedia instructions to microprocessors, facilitating ubiquitous and pervasive multimedia. She co-led an Intel-HP architecture team designing new ISA for multimedia and data parallelism for 64-bit Intel microprocessors. Simultaneous with
her full-time HP tenure, she was also Consulting Professor of Electrical Engineering at Stanford University. She has a Ph.D. in Electrical Engineering and a M.S. in Computer Science, both from Stanford University, and an A.B. with distinction from Cornell University, where she was a College Scholar. She has been granted over 120 United States and international patents, and has authored numerous conference and journal papers on computer architecture, processor design, multimedia and security topics.
Keynote 2:
The Art of Application-Specific Processor Design: Great Artists use Good Tools, Gert Goossens

Abstract

Application-Specific Processors (ASIPs) are clearly becoming accepted as key building blocks of multi-core systems-on-chip that power today's electronic systems. In this presentation, we will review methodologies for the design of ASIPs.

We believe that retargetable software tools are an absolute prerequisite for contemporary ASIP design. A central element of such a tool flow is a retargetable C compiler that drives the architectural exploration process.

Retargetable software tools introduce formalism and correctness, eliminate guess work, and extend the designer's capabilities beyond the architectural limitations of configurable processor templates as offered by intellectual property vendors. They enable the creation of differentiating intellectual property, fully supported by C-based software development tools and automatically generated RTL hardware implementations.

Speaker's Bio

Gert Goossens is the CEO and a co-founder of Target Compiler Technologies, a provider of retargetable tools for the design of application-specific processors. Before founding Target in 1996, Gert Goossens was affiliated with the IMEC research centre, where he headed research groups on behavioural synthesis and software compilation. Gert Goossens holds several patents in the area of processor modelling and design, and has authored or co-authored around 40 papers in electronic design automation. He received a masters and a Ph.D. degree in electrical engineering from K.U. Leuven, in 1984 and 1989 respectively.