Message from the Conference Chairs p. ix
Conference Committee p. x
Keynote
Defect-Tolerant Molecular Electronics p. 2
Scheduling and Codesign
Modeling and Scheduling Parallel Data Flow Systems Using Structured Systems of Recurrence Equations p. 6
Resource Constrained and Speculative Scheduling of an Algorithm Class with Run-Time Dependent Conditionals
CHARMED: A Multi-objective Co-synthesis Framework for Multi-mode Embedded Systems p. 28
Reliability-Aware Co-synthesis for Embedded Systems p. 41
Arithmetic I
Complex Square Root with Operand Prescaling p. 52
Parallel Montgomery Multipliers p. 63
Improved-Throughput Networks of Basic On-line Arithmetic Modules for DSP Applications p. 73
Decimal Floating-Point Division Using Newton-Raphson Iteration p. 84
Instruction Set Extensions
A Public-key Cryptographic Processor for RSA and ECC p. 98
Architectural Support for Arithmetic in Optimal Extension Fields p. 111
Evaluating Instruction Set Extensions for Fast Arithmetic on Binary Finite Fields p. 125
Efficient Processing of Color Image Sequences Using a Color-Aware Instruction Set on Mobile Systems p. 137
(Special) Nanocomputing
Binary Multiplication Based on Single Electron Tunneling p. 152
A Novel Highly Reliable Low-Power Nano Architecture When von Neumann Augments Kolmogorov p. 167
Microarchitecture, Compilers and Optimization
Register Organization for Enhanced On-Chip Parallelism p. 180
Design and Evaluation of a Network-Based Asynchronous Architecture for Cryptographic Devices p. 191
Common Subexpression Elimination Involving Multiple Variables for Linear DSP Synthesis p. 202
Optimizing the Memory Bandwidth with Loop Morphing p. 213
Switching-Activity Minimization on Instruction-level Loop Scheduling for VLIW DSP Applications p. 224
Arithmetic II
A Digit-Serial Algorithm for the Discrete Logarithm Modulo 2[^k] p. 236
An Algorithm and Hardware Architecture for Integrated Modular Division and Multiplication in GF(p) and GF(2[^n]) p. 247
Detecting Faults in Four Symmetric Key Block Ciphers p. 258
A Low-Power Carry Skip Adder with Fast Saturation p. 269
Communication, Interfaces and Memory