Table of Contents for Proceedings
ARITH-16

Foreword viii

Dedication ix

Committees x

Additional Reviewers xii

Session 1: Keynote Talk
Chair: Jean-Claude Bajard

Computer Arithmetic — An Algorithm Engineer's Perspective 2
D. Matula

Session 2: Multiplication
Chair: Luigi Dadda

High-Performance Left-to-Right Array Multiplier Design 4
Z. Huang and M. Ercegovac

Multiple-Precision Fixed-Point Vector Multiply-Accumulator Using Shared Segmentation 12
D. Tan, A. Danysh, and M. Liebelt

Some Optimizations of Hardware Multiplication by Constant Matrices 20
N. Boullis and A. Tisserand

A Less Recursive Variant of Karatsuba-Ofman Algorithm for Multiplying Operands of Size a Power of Two 28
S. Erdem and Ç. Koç

Session 3: Division
Chair: Paolo Montuschi

Revisiting SRT Quotient Digit Selection 38
P. Kornerup

SRT Division Algorithms as Dynamical Systems 46
M. McCann and N. Pippenger

A New Iterative Structure for Hardware Division: the Parallel Paths Algorithm 54
E. Rice and R. Hughey

Prescaled Integer Division 63
D. Matula and A. Fit-Florea

Session 4: Floating Point
Chair: Andrew Beaumont-Smith

Hardware Implementations of Denormalized Numbers 70
E. Schwarz, M. Schmookler, and S. Trong

Representable Correcting Terms for Possibly Underflowing Floating Point Operations 79
S. Boldo and M. Daumas

High Performance Floating-Point Unit with 116 Bit Wide Divider 87
G. Gerwig, H. Wetter, E. Schwarz, and J. Haess

The Case for a Redundant Format in Floating Point Arithmetic 95
H. Fahmy and M. Flynn

Session 5: Decimal Arithmetic and Revisions to the IEEE 754 Standard
Chair: Eric Schwarz

Decimal Floating-Point: Algorism for Computers.....104
M. Cowlishaw

Panel: Revisions to the IEEE 754 Standard for Floating-Point Arithmetic 112
E. Schwarz

Session 6: Elementary Functions
Chair: Renato Stefanelli, Politecnico de Milano

"Partially Rounded" Small-Order Approximations for Accurate, Hardware-Oriented, Table-Based Methods 114
J.-M. Muller

An Overview of Floating-Point Support and Math Library on the Intel® XScale™ Architecture 122
C. Iordache and P. Tang

Theorems on Efficient Argument Reductions 129
R.-C. Li, S. Boldo, and M. Daumas

Accelerating Sine and Cosine Evaluation with Compiler Assistance.....137
P. Markstein

Session 7: Testing and Error Analysis
Chair: Tanya Vladimirova

Worst Cases and Lattice Reduction 142
D. Stehlé, V. Lefèvre, and P. Zimmermann

Isolating Critical Cases for Reciprocals Using Integer Factorization 148
J. Harrison

Solving Range Constraints for Binary Floating-Point Instructions 158
A. Ziv, M. Aharoni, and S. Asaf

A Parametric Error Analysis of Goldschmidt's Division Algorithm 165
G. Even, P.-M. Seidel, and W. Ferguson

Session 8: Cryptography
Chair: Peter Montgomery

A Unidirectional Bit Serial Systolic Architecture for Double-Basis Division over GF(2^m).....174
A. Daneshbeh and A. Hasan

Efficient Multiplication in $GF(p^k)$ for Elliptic Curve Cryptography 181
J.-C. Bajard, L. Imbert, C. Nègre, and T. Plantard

Low Complexity Sequential Normal Basis Multipliers over $GF(2^m)$.....188
A. Reyhani-Masoleh and A. Hasan

A Low Complexity and a Low Latency Bit Parallel Systolic Multiplier over $GF(2^m)$ Using an Optimal Normal Basis of Type II 196
S. Kwon

Session 9: Powering, Multiplication, and Counters
Chair: Alexandre Tenca

High-Radix Iterative Algorithm for Powering Computation 204
J.-A. Piñeiro, M. Ercegovac, and J. Bruguera

On-Line Multiplication in Real and Complex Base 212
C. Frougny and A. Surarerks

A VLSI Algorithm for Modular Multiplication/Division 220
M. Kaihara and N. Takagi

Saturating Counters: Application and Design Alternatives 228
I. Koren, Y. Koren, and B. Oomman

Session 10: Number Systems
Chair: Colin Walter, Comodo Research Labs

Error-Free Arithmetic for Discrete Wavelet Transforms Using Algebraic Integers 238
K. Wahid, V. Dimitrov, and G. Jullien

On Computing Addition Related Arithmetic Operations via Controlled Transport of Charge 245
C. Cotofana, C. Lageweg, and S. Vassiliadis

The Interval Logarithmic Number System 253
M. Arnold, J. Garcia, and M. Schulte

Scaling an RNS Number Using the Core Function 262
N. Burgess

Session 11: Modeling and Design of Arithmetic Components
Chair: Peter-Michael Seidel

Energy-Delay Estimation Technique for High-Performance Microprocessor VLSI Adders 272
V. Oklobdzija, B. Zeydel, H. Dao, S. Mathew, and R. Krishnamurthy

Tutorial: Design of Power Efficient VLSI Arithmetic: Speed and Power Trade-offs 280
V. Oklobdzija and R. Krishnamurthy

Author Index 281