# Table of Contents


**14th Symposium on Computer Arithmetic**

**Foreword** ..... viii

**Symposium Committee** ..... ix

**Program Committee** ..... x

**List of Reviewers** ..... xi

**Invited Talk**

***Chair:*** *Israel Koren*

Computer Arithmetic — A Programmer's Perspective ..... 2
*Richard P. Brent, Oxford University*

**Processor Enhancements**

***Chair:*** *Peter Kornerup*

New Algorithms for Improved Transcendental Functions on IA-64 ..... 4
*S. Story and P.T.P. Tang*

A Low-Power, High-Speed Implementation of a PowerPC™ Microprocessor Vector Extension ..... 12
*M.S. Schmookler, M. Putrino, A. Mather, J. Tyler, H.V. Nguyen, C. Roth, M. Sharma, M.N. Pham, and J. Lent*

**Addition**

***Chair:*** *Neil Weste*

Intermediate Variable Encodings that Enable Multiplexor-Based Implementations of Two Operand Addition ..... 22
*D.S. Phatak and I. Koren*

A Family of Adders ..... 30
*S. Knowles*

Reduced Latency IEEE Floating-Point Standard Adder Architectures ..... 35
*A. Beaumont-Smith, N. Burgess, S. Lefrere, and C.C. Lim*

**Division**

***Chair:*** *Renato Stefanelli*

On the Design of High-Radix On-Line Division for Long Precision ..... 44
*A.F. Tenca and M.D. Ercegovac*

Boosting Very-High Radix Division with Prescaling and Selection by Rounding ..... 52
*P. Montuschi and T. Lang*

Low-Power Division: Comparison among Implementations of Radix 4, 8 and 16 ..... 60
*A. Nannarelli and T. Lang*

**Cryptography and Graphics**

***Chair:*** *Milos Ercegovac*

Montgomery Modular Exponentiation on Reconfigurable Hardware ..... 70
*T. Blum and C. Paar*

Moduli for Testing Implementations of the RSA Cryptosystem ..... 78
*C.D. Walter*

Digit-Recurrence Algorithm for Computing Euclidean Norm of a 3-D Vector ..... 86
*N. Takagi and S. Kuwahara*

**Divide and Square Root**

***Chair:*** *Atsuki Inoue*

Correctness Proofs Outline for Newton-Raphson Based Floating-Point Divide and Square Root Algorithms ..... 96
*M.A. Cornea-Hasegan, R.A. Golliver, and P. Markstein*

Floating Point Division and Square Root Algorithms and Implementation in the AMD-K7™ Microprocessor ..... 106
*S.F. Oberman*

Series Approximation Methods for Divide and Square Root in the Power3™ Processor ..... 116
*R.C. Agarwal, F.G. Gustavson, and M.S. Schmookler*

High-Speed Inverse Square Roots ..... 124
*M.J. Schulte and K.E. Wires*

**Number Systems**

***Chair:*** *Colin Walter*

Arithmetic with Signed Analog Digits ..... 134
*A. Saed, M. Ahmadi, and G.A. Jullien*

A 32-Bit Logarithmic Arithmetic Unit and Its Performance Compared to Floating-Point ..... 142
*J.N. Coleman and E.I. Chester*

Necessary and Sufficient Conditions for Parallel, Constant Time Conversion and Addition ..... 152
*P. Kornerup*

**Residue Number Systems**

***Chair:*** *Graham Jullien*

Efficient VLSI Implementation of Modulo $(2^n \pm 1)$ Addition and Multiplication ..... 158
*R. Zimmermann*

A Reverse Converter for the 4-Moduli Superset $\{2^n-1, 2^n, 2^n+1, 2^{n+1}+1\}$ ..... 168
*M. Bhardwaj, T. Srikanthan, and C.T. Clarke*

VLSI Costs of Arithmetic Parallelism: A Residue Reverse Conversion Perspective ..... 176
*M. Bhardwaj, T. Srikanthan, and C.T. Clarke*

**CORDIC Algorithms**

***Chair:*** *Jeong Lee*

Interval Sine and Cosine Functions Computation Based on Variable-Precision CORDIC Algorithm ..... 186
*J. Hormigo, J. Villalba, and E.L. Zapata*

Complex Logarithmic Number System Arithmetic Using High-Radix Redundant CORDIC Algorithms ..... 194
*D. Lewis*

Very-High Radix CORDIC Vectoring with Scalings and Selection by Rounding ..... 204
*E. Antelo, T. Lang, and J.D. Bruguera*

**Multiplication and Rounding**

***Chair:*** *William McAllister*

Area x Delay ($A \cdot T$) Efficient Multipliers Based on an Intermediate Hybrid Signed-Digit (HSD-1) Representation ..... 216
*J.-J.J. Lue and D.S. Phatak*

A Comparison of Three Rounding Algorithms for IEEE Floating-Point Multiplication ..... 225
*G. Even and P.-M. Seidel*

On Infinitely Precise Rounding for Division, Square Root, Reciprocal and Square Root Reciprocal ..... 233
*C. Iordache and D.W. Matula*

Number-Theoretic Test Generation for Directed Rounding ..... 241
*M. Parks*

**Floating Point**

***Chair:*** *Stuart F. Oberman*

Multiplications of Floating Point Expansions ..... 250
*M. Daumas*

The S/390 G5 Floating Point Unit Supporting Hex and Binary Architectures ..... 258
*E.M. Schwarz, R.M. Smith, and C.A. Krygowski*

Floating-Point Unit in Standard Cell Design with 116 bit Wide Dataflow ..... 266
*G. Gerwig and M. Kroener*

**Author Index** ..... 274