

2015 IEEE 22nd Symposium on Computer Arithmetic

(ARITH 2015)

**Lyon, France
22-24 June 2015**



**IEEE Catalog Number: CFP15121-POD
ISBN: 978-1-4799-8665-1**

2015 IEEE 22nd Symposium on Computer Arithmetic

ARITH 2015

Table of Contents

Foreword.....	viii
Organizing Committee.....	ix
Program Committee.....	x
Steering Committee.....	xii

Session 1: Keynote Talk

Calculating in Floating Sexagesimal Place Value Notation, 4000 years ago	1
<i>Christine Proust</i>	

Session 2: Arithmetic Units 1

Low-Cost Duplicate Multiplication	2
<i>Michael B. Sullivan and Earl E. Swartzlander</i>	
Minimizing Energy by Achieving Optimal Sparseness in Parallel Adders	10
<i>Mustafa Aktan, Dursun Baran, and Vojin G. Oklobdzija</i>	

Session 3: Arithmetic Units 2

An Efficient Softcore Multiplier Architecture for Xilinx FPGAs	18
<i>Martin Kumm, Shahid Abbas, and Peter Zipf</i>	
Design and Implementation of an Embedded FPGA Floating Point DSP Block	26
<i>Martin Langhammer and Bogdan Pasca</i>	

Session 4: Elementary and Special Functions 1

Hardware Implementations of Fixed-Point Atan2	34
<i>Florent de Dinechin and Matei Istoan</i>	
A General-Purpose Method for Faithfully Rounded Floating-Point Function Approximation in FPGAs	42
<i>David B. Thomas</i>	

Session 5: Elementary and Special Functions 2

Precise and Fast Computation of Elliptic Integrals and Functions	50
<i>Toshio Fukushima</i>	
Semi-Automatic Floating-Point Implementation of Special Functions	58
<i>Christoph Lauter and Marc Mezzarobba</i>	
Code Generators for Mathematical Functions	66
<i>Nicolas Brunie, Florent de Dinechin, Olga Kupriianova, and Christoph Lauter</i>	

Session 6: Keynote Talk

The End of Numerical Error	74
<i>John Gustafson</i>	

Session 7: Medium and Multiple Precision 1

Faster FFTs in Medium Precision	75
<i>Joris van der Hoeven and Grégoire Lecerf</i>	
Efficient Implementation of Elementary Functions in the Medium-Precision Range	83
<i>Fredrik Johansson</i>	

Session 8: Medium and Multiple Precision 2

Efficient Divide-and-Conquer Multiprecision Integer Division	90
<i>William Bruce Hart</i>	
Reliable Evaluation of the Worst-Case Peak Gain Matrix in Multiple Precision	96
<i>Anastasia Volkova, Thibault Hilaire, and Christoph Lauter</i>	

Session 9: Keynote Talk

Numerical Challenges in Long Term Integrations of the Solar System	104
<i>Jacques Laskar</i>	

Session 10: Residue Number Systems

Contributions to the Design of Residue Number System Architectures	105
<i>Benoît Gérard, Jean-Gabriel Kammerer, and Nabil Merkiche</i>	
RNS Arithmetic Approach in Lattice-Based Cryptography: Accelerating the “Rounding-off” Core Procedure	113
<i>Jean-Claude Bajard, Julien Eynard, Nabil Merkiche, and Thomas Plantard</i>	

Session 11: Modular and Finite-Field Arithmetic

Modulo- $(2^n - 2^q - 1)$ Parallel Prefix Addition via Excess-Modulo Encoding of Residues	121
<i>Seyed Hamed Fatemi Langroudi and Ghassem Jaberipur</i>	
New Bit-Level Serial GF (2^m) Multiplication Using Polynomial Basis	129
<i>Hayssam El-Razouk and Arash Reyhani-Masoleh</i>	
Modular Multiplication and Division Algorithms Based on Continued Fraction Expansion	137
<i>Mourad Gouicem</i>	
Efficient Modular Exponentiation Based on Multiple Multiplications by a Common Operand	144
<i>Christophe Negre, Thomas Plantard, and Jean-Marc Robert</i>	

Session 12: Miscellaneous

Reproducible Tall-Skinny QR	152
<i>Hong Diep Nguyen and James Demmel</i>	
An Automatable Formal Semantics for IEEE-754 Floating-Point Arithmetic	160
<i>Martin Brain, Cesare Tinelli, Philipp Riemmer, and Thomas Wahl</i>	
The Exact Real Arithmetical Algorithm in Binary Continued Fractions	168
<i>Petr Kurka</i>	
Author Index	176