

2013 IEEE 21st Symposium on Computer Arithmetic

(ARITH 2013)

**Austin, Texas, USA
7 – 10 April 2013**



**IEEE Catalog Number: CFP13121-PRT
ISBN: 978-1-4673-5644-2**

2013 21st IEEE Symposium on Computer Arithmetic

ARITH-21

Table of Contents

Foreword.....	viii
Dedication.....	ix
Steering Committee.....	xii
Symposium Committee.....	xiii
Program Committee.....	xiv
Additional Reviewers.....	xv
Corporate Sponsors.....	xvi

Session 1: Keynote Talk I

Session Chair: David W. Matula

High-Precision Computation: Applications and Challenges	3
<i>David H. Bailey</i>	

Session 2: Arithmetic Units

Session Chair: Stuart Oberman

The Floating-Point Unit of the Jaguar x86 Core	7
<i>Jeff Rupley, John King, Eric Quinnell, Frank Galloway, Ken Patton, Peter-Michael Seidel, James Dinh, Hai Bui, and Anasua Bhowmik</i>	
Split-Path Fused Floating Point Multiply Accumulate (FPMAC)	17
<i>Suresh Srinivasan, Ketan Bhudiya, Rajaraman Ramanarayanan, P. Sahit Babu, Tiju Jacob, Sanu K. Mathew, Ram Krishnamurthy, and Vasantha Errgauntla</i>	
FPU Generator for Design Space Exploration	25
<i>Sameh Galal, Ofer Shacham, John S. Brunhaver II, Jing Pu, Artem Vassiliev, and Mark Horowitz</i>	

Session 3: Special Session on Exascale Computing

Session Chair: Eric Schwarz

Managing Computation, Precision, Accuracy and Performance on ExaScale Systems	37
--	----

Session 4: Domain Specific Designs

Session Chair: Paolo Montuschi

Improved Architectures for a Floating-Point Fused Dot Product Unit	41
<i>Jongwook Sohn and Earl E. Swartzlander</i>	
Floating Point Architecture Extensions for Optimized Matrix Factorization	49
<i>Ardavan Pedram, Andreas Gerstlauer, and Robert A. van de Geijn</i>	
A Fast Circuit Topology for Finding the Maximum of N k-bit Numbers	59
<i>Bilgiday Yuces, H. Fatih Ugurdag, Sezer Gören, and Gunhan Dundar</i>	
A Non-Linear/Linear Instruction Set Extension for Lightweight Ciphers	67
<i>Susanne Engels, Elif Bilge Kavun, Christof Paar, Tolga Yalçin, and Hristina Mihajloska</i>	

Session 5: Keynote Talk II

Session Chair: Neil Burgess

The Antikythera Mechanism and the Early History of Mechanical Computing	79
<i>M.G. Edmunds</i>	

Session 6: Verification and Correctness Proofs

Session Chair: David Hough

On the Componentwise Accuracy of Complex Floating-Point Division with an FMA	83
<i>Claude-Pierre Jeannerod, Nicolas Louvet, and Jean-Michel Muller</i>	
How to Compute the Area of a Triangle: A Formal Revisit	91
<i>Sylvie Boldo</i>	
SIPE: Small Integer Plus Exponent	99
<i>Vincent Lefèvre</i>	
A Formally-Verified C Compiler Supporting Floating-Point Arithmetic	107
<i>Sylvie Boldo, Jacques-Henri Jourdan, Xavier Leroy, and Guillaume Melquiond</i>	

Session 7: Modular Arithmetic

Session Chair: Peter Kornerup

Fault Detection in RNS Montgomery Modular Multiplication	119
<i>Jean-Claude Bajard, Julien Eynard, and Filippo Gandino</i>	
The Unary Arithmetical Algorithm in Bimodular Number Systems	127
<i>Petr Kůrka and Martin Delacourt</i>	
Parallel Modular Multiplication on Multi-core Processors	135
<i>Pascal Giorgi, Laurent Imbert, and Thomas Izard</i>	

Session 8: Floating-Point Error Analysis

Session Chair: Sanu Mathew

Comparison between Binary64 and Decimal64 Floating-Point Numbers	145
<i>Nicolas Brisebarre, Marc Mezzarobba, Jean-Michel Muller, and Christoph Lauter</i>	
Accurate Parallel Floating-Point Accumulation	153
<i>Edin Kadric, Paul Gurniak, and André Dehon</i>	
Fast Reproducible Floating-Point Summation	163
<i>James Demmel and Hong Diep Nguyen</i>	

Session 9: Function Approximation

Session Chair: Debjit DasSarma

Multiple-Precision Evaluation of the Airy A_i Function with Reduced Cancellation	175
<i>Sylvain Chevillard and Marc Mezzarobba</i>	
Accurate and Fast Evaluation of Elementary Symmetric Functions	183
<i>Hao Jiang, Stef Graillat, and Roberto Barrio</i>	
Truncated Logarithmic Approximation	191
<i>Michael B. Sullivan and Earl E. Swartzlander</i>	

Session 10: Arithmetic in Cryptography

Session Chair: Naofumi Takagi

Relation Collection for the Function Field Sieve	201
<i>Jérémie Detrey, Pierrick Gaudry, and Marion Videau</i>	
Another Look at Inversions over Binary Fields	211
<i>Vassil Dimitrov and Kimmo Järvinen</i>	
On-the-Fly Multi-base Recoding for ECC Scalar Multiplication without Pre-computations	219
<i>Thomas Chabrier and Arnaud Tisserand</i>	

Special Session

Precision, Accuracy, and Rounding Error Propagation in Exascale Computing	231
<i>Marius Cornea</i>	
Numerical Reproducibility and Accuracy at ExaScale	235
<i>James Demmel and Hong Diep Nguyen</i>	
Author Index	238