

2016 IEEE 23rd Symposium on Computer Arithmetic (ARITH 2016)

**Silicon Valley, California, USA
10-13 July 2016**



**IEEE Catalog Number: CFP16121-POD
ISBN: 978-1-5090-1617-4**

**Copyright © 2016 by the Institute of Electrical and Electronics Engineers, Inc
All Rights Reserved**

Copyright and Reprint Permissions: Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

For other copying, reprint or republication permission, write to IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854. All rights reserved.

******This publication is a representation of what appears in the IEEE Digital Libraries. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number:	CFP16121-POD
ISBN (Print-On-Demand):	978-1-5090-1617-4
ISBN (Online):	978-1-5090-1616-7
ISSN:	1063-6889

Additional Copies of This Publication Are Available From:

Curran Associates, Inc
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: (845) 758-0400
Fax: (845) 758-2633
E-mail: curran@proceedings.com
Web: www.proceedings.com

CURRAN ASSOCIATES INC.
proceedings
.com

2016 IEEE 23rd Symposium on Computer Arithmetic

ARITH 2016

Table of Contents

Foreword.....	viii
Committees.....	xi
Reviewers.....	xiv
Keynote Talks and Special Sessions.....	xv

Session 1: Arithmetic Units

Efficient Combinational Circuits for Division by Small Integer Constants	1
<i>H. Fatih Ugurdag, Anil Bayram, Vecdi Emre Levent, and Sezer Gören</i>	
A Formulation of Fast Carry Chains Suitable for Efficient Implementation with Majority Elements	8
<i>Ghassem Jaberipur, Behrooz Parhami, and Dariush Abedi</i>	

Session 2: Security and Cryptography (I)

Multi-fault Attack Detection for RNS Cryptographic Architecture	16
<i>Jean-Claude Bajard, Julien Eynard, and Nabil Merkiche</i>	
A CRC-Based Concurrent Fault Detection Architecture for Galois/Counter Mode (GCM)	24
<i>Amir Ali Kouzeh Geran and Arash Reyhani-Masoleh</i>	

Session 3: Big Numbers

Accelerating Big Integer Arithmetic Using Intel IFMA Extensions	32
<i>Shay Gueron and Vlad Krasnov</i>	
A New Multiplication Algorithm for Extended Precision Using Floating-Point Expansions	39
<i>Jean-Michel Muller, Valentina Popescu, and Ping Tak Peter Tang</i>	
Optimizing Modular Multiplication for NVIDIA's Maxwell GPUs	47
<i>Niall Emmart, Justin Luitjens, Charles Weems, and Cliff Woolley</i>	

Session 4: Accuracy and Reproducibility

Verificarlo: Checking Floating Point Accuracy through Monte Carlo Arithmetic	55
<i>Christophe Denis, Pablo de Oliveira Castro, and Eric Petit</i>	
Recovering Numerical Reproducibility in Hydrodynamic Simulations	63
<i>Philippe Langlois, Rafife Nheili, and Christophe Denis</i>	
Correctly Rounded Arbitrary-Precision Floating-Point Summation	71
<i>Vincent Lefèvre</i>	

Session 5: Floating-Point Implementations

Digit Recurrence Floating-Point Division under HUB Format	79
<i>Julio Villalba-Moreno</i>	
Quad Precision Floating Point on the IBM z13™	87
<i>Cedric Lichtenau, Steven Carlough, and Silvia Melitta Mueller</i>	

Session 6: Less-conventional Number Systems (I)

Accuracy and Performance Trade-Offs of Logarithmic Number Units in Multi-Core Clusters	95
<i>Michael Schaffner, Michael Gautschi, Frank K. Gürkaynak, and Luca Benini</i>	
An Iterative Logarithmic Multiplier with Improved Precision	104
<i>Syed Ershad Ahmed, Sanket Kadam, and M. B. Srinivas</i>	

Session 7: Security and Cryptography (II)

Hardware Implementation of AES Using Area-Optimal Polynomials for Composite-Field Representation $GF(2^4)^2$ of $GF(2^8)$	112
<i>Shay Gueron and Sanu Mathew</i>	
Random Digit Representation of Integers	118
<i>Nicolas Méloni and M. Anwar Hasan</i>	
Hybrid Position-Residues Number System	126
<i>Karim Bigou and Arnaud Tisserand</i>	

Session 8: Less-conventional Number Systems (II)

On-line Multiplication and Division in Real and Complex Bases	134
<i>Marta Brzicová, Christiane Frougny, Edita Pelantová, and Milena Svobodová</i>	
Evaluating Straight-Line Programs over Balls	142
<i>Joris van der Hoeven and Grégoire Lecerf</i>	
A Parallel Decimal Multiplier Using Hybrid Binary Coded Decimal (BCD) Codes	150
<i>Xiaoping Cui, Weiqiang Liu, Dong Wenwen, and Fabrizio Lombardi</i>	

Session 9: Logarithm Implementations

Computing floating-point logarithms with fixed-point operations	156
<i>Julien Le Maire, Nicolas Brunie, Florent de Dinechin, and Jean-Michel Muller</i>	
Single Precision Natural Logarithm Architecture for Hard Floating-Point and DSP-Enabled FPGAs	164
<i>Martin Langhammer and Bogdan Pasca</i>	
Automated Design of Floating-Point Logarithm Functions on Integer Processors	172
<i>Guillaume Revy</i>	
Author Index	181