

# **2024 IEEE 31st Symposium on Computer Arithmetic (ARITH 2024)**

**Malaga, Spain  
10 – 12 June 2024**



**IEEE Catalog Number: CFP24121-POD  
ISBN: 979-8-3503-8433-8**

**Copyright © 2024 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 is a print representation of what appears in the IEEE Digital Library. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number:	CFP24121-POD
ISBN (Print-On-Demand):	979-8-3503-8433-8
ISBN (Online):	979-8-3503-8432-1
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](mailto:curran@proceedings.com)  
Web: [www.proceedings.com](http://www.proceedings.com)

CURRAN ASSOCIATES INC.  
**proceedings**  
.com

# 2024 IEEE 31st Symposium on Computer Arithmetic (ARITH) **ARITH 2024**

## Table of Contents

Message from Conference Chairs .....	viii
Organizing Committee .....	x
Program Committee .....	xi
Steering Committee .....	xii
Reviewers .....	xiv
Sponsors .....	xvi

### Arithmetic for Cryptography #1

Hardware Acceleration of the Prime-Factor and Rader NTT for BGV Fully Homomorphic Encryption .....	1
<i>David Du Pont (KU Leuven, Belgium), Jonas Bertels (COSIC, KU Leuven, Belgium), Furkan Turan (COSIC, KU Leuven, Belgium), Michiel Van Beirendonck (COSIC, KU Leuven, Belgium), and Ingrid Verbauwhede (COSIC, KU Leuven, Belgium)</i>	
PQC-AMX: Accelerating Saber and FrodoKEM on the Apple M1 and M3 SoCs .....	9
<i>Décio Luiz Gazzoni Filho (Universidade Estadual de Campinas (UNICAMP), Brazil; State University of Londrina, Brazil), Guilherme Brandão (Independent Researcher, Brazil), Gora Adj (Cryptography Research Centre, Technology Innovation Institute, Abu Dhabi, UAE), Arwa Alblooshi (Cryptography Research Centre, Technology Innovation Institute, Abu Dhabi, UAE), Isaac A. Canales-Martínez (Cryptography Research Centre, Technology Innovation Institute, Abu Dhabi, UAE), Jorge Chávez-Saab (Cryptography Research Centre, Technology Innovation Institute, Abu Dhabi, UAE), and Julio López (Universidade Estadual de Campinas (UNICAMP), Campinas, Brazil)</i>	
Montgomery Modular Multiplication via Single-Base Residue Number Systems .....	17
<i>Zabihollah Ahmadpour (Shahid Beheshti University, Iran), Ghassem Jaberipur (Chosun University, Republic of Korea), and Jeong-A Lee (Chosun University, Republic of Korea)</i>	

### Datapath Design I #2

Combining Power and Arithmetic Optimization via Datapath Rewriting .....	24
<i>Samuel Coward (Intel Corporation; Imperial College London), Theo Drane (Intel Corporation), Emiliano Morini (Intel Corporation), and George A. Constantinides (Imperial College London)</i>	

Useful Applications of Correctly-Rounded Operators of the Form $ab + cd + e$ .....	32
<i>Tom Hubrecht (PSL University, France), Claude-Pierre Jeannerod (Inria, Univ. Lyon, France), and Jean-Michel Muller (CNRS, Univ. Lyon, France)</i>	
Fused FP8 4-Way Dot Product with Scaling and FP32 Accumulation .....	40
<i>David R. Lutz (Arm Ltd., US), Anisha Saini (Arm Ltd., US), Mairin Kroes (Arm Ltd., UK), Thomas Elmer (Arm Ltd., US), and Harsha Valsaraju (Arm Ltd., US)</i>	

## Datapath Design II #3

Multiple-Base Logarithmic Quantization and Application in Reduced Precision AI Computations .....	48
<i>Vassil Dimitrov (Lemurian Labs, Canada; University of Calgary, Canada), Richard Ford (Lemurian Labs, Canada), Laurent Imbert (Lemurian Labs, Canada; University of Montpellier, France), Arjuna Madanayake (Lemurian Labs, Canada), Nilan Udayanga (Lemurian Labs, Canada), and Will Wray (Lemurian Labs, Canada)</i>	
Novel Access Patterns Based on Overlapping Loading and Processing Times to Reduce Latency and Increase Throughput in Memory-Based FFTs .....	52
<i>Zeynep Kaya (Bilecik Seyh Edebali University, Türkiye) and Mario Garrido (Universidad Politécnica de Madrid, Spain)</i>	

## Math Tools, Libraries and Software Evaluation #4

An Open-Source RISC-V Vector Math Library .....	60
<i>Ping Tak Peter Tang (Rivos Inc., Santa Clara)</i>	
MATLAB Simulator of Level-Index Arithmetic .....	68
<i>Mantas Mikaitis (University of Leeds, United Kingdom)</i>	
APyTypes: Algorithmic Data Types in Python for Efficient Simulation of Finite Word-Length Effects .....	72
<i>Mikael Henriksson (Linköping University, Sweden), Theodor Lindberg (Linköping University, Sweden), and Oscar Gustafsson (Linköping University, Sweden)</i>	
An Emacs-Cairo Scrolling Bug Due to Floating-Point Inaccuracy .....	76
<i>Vincent Lefèvre (Univ Lyon, EnsL, UCBL, CNRS, Inria, France)</i>	

## Transcendental Functions and Error Analysis #5

Fast Multiple Precision $\exp(x)$ with Precomputations .....	80
<i>Joris van der Hoeven (CNRS, LIX (UMR 7161), France) and Fredrik Johansson (Inria, IMB (UMR 5251), France)</i>	
HGH-CORDIC: A High-Radix Generalized Hyperbolic Coordinate Rotation Digital Computer .....	88
<i>Hui Chen (Nanjing University of Aeronautics and Astronautics, China), Lianghua Quan (Nanjing University, China), and Weiqiang Liu (Nanjing University of Aeronautics and Astronautics, China)</i>	

Rounding Error Analysis of an Orbital Collision Probability Evaluation Algorithm .....	96
<i>Denis Arzelier (LAAS-CNRS, France), Florent Bréhard (Univ. Lille, CNRS, CRIStAL, France), Mioara Joldes (LAAS-CNRS, France), and Marc Mezzarobba (LIX, CNRS, France)</i>	

## Arithmetic Operators #6

Multiplier Architecture with a Carry-Based Partial Product Encoding .....	104
<i>Martin Langhammer (Intel Corporation, UK), Bogdan Pasca (Intel Corporation, France), and Igor Kucherenko (Intel Corporation, US)</i>	
On the Systematic Creation of Faithfully Rounded Commutative Truncated Booth Multipliers .....	108
<i>Theo Drane (Intel Corporation), Samuel Coward (Intel Corporation), Mertcan Temel (Intel Corporation), and Joe Leslie-Hurd (Intel Corporation)</i>	
A Time Efficient Comprehensive Model of Approximate Multipliers for Design Space Exploration .....	116
<i>Ziying Cui (Nanjing University of Aeronautics and Astronautics, China), Ke Chen (Nanjing University of Aeronautics and Astronautics, China), Bi Wu (Nanjing University of Aeronautics and Astronautics, China), Chenggang Yan (Nanjing University of Aeronautics and Astronautics, China), Yu Gong (Nanjing University of Aeronautics and Astronautics, China), and Weiqiang Liu (Nanjing University of Aeronautics and Astronautics, China)</i>	
Small Logic-Based Multipliers with Incomplete Sub-Multipliers for FPGAs .....	124
<i>Andreas Boettcher (Fulda University of Applied Sciences, Germany) and Martin Kumm (Fulda University of Applied Sciences, Germany)</i>	

## Alternative Formats #7

Square Root Unit with Minimum Iterations for Posit Arithmetic .....	132
<i>Raul Murillo (Complutense University of Madrid, Spain), Alberto A. Del Barrio (Complutense University of Madrid, Spain), and Guillermo Botella (Complutense University of Madrid, Spain)</i>	
PT-Float: A Floating-Point Unit with Dynamically Varying Exponent and Fraction Sizes .....	139
<i>José T. de Sousa (INESC-ID/IST/UL), João D. Lopes (INESC-ID/IST/UL), Micaela Serôdio (INESC-ID/IST/UL), Horácio C. Neto (INESC-ID/IST/UL), and Mário P. Véstias (INESC-ID/ISEL/IPL)</i>	

<b>Author Index</b> .....	<b>147</b>
---------------------------	------------