2021 IEEE 28th Symposium on Computer Arithmetic (ARITH 2021)

Virtual Conference
14-16 June 2021

IEEE Catalog Number: CFP21121-POD
ISBN: 978-1-6654-4648-8

Copyright © 2021 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:	CFP21121-POD
ISBN (Print-On-Demand):	978-1-6654-4648-8
ISBN (Online):	978-1-6654-2293-2
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

2021 IEEE 28th Symposium on Computer Arithmetic (ARITH)

ARITH 2021

Table of Contents

Foreword ix

Organizing Committee xi

Program Committee xii

Steering Committee xiii

External Reviewers xiv

Industry Panel xv

Keynotes xvi

Sponsors xviii

Session 1: Precision tuning and verification

Combining Precision Tuning and Rewriting 1
Brett Saiki (University of Washington, USA), Oliver Flatt (University of Utah, USA), Chandrakana Nandi (University of Washington, USA), Pavel Panchekha (University of Utah, USA), and Zachary Tatlock (University of Washington, USA)

Tagged Error: Tracing Numerical Error through Computations 9
Nestor Demeure (Université Paris-Saclay, CNRS, ENS Paris-Saclay, France), Cedric Chevalier (Université Paris-Saclay, CEA, France), Christophe Denis (Sorbonne Université, CNRS, France), and Pierre Dossantos-Uzarralde (CEA, DAM, DIF, France)

Session 2: Floating point error analysis

a • (x • x) or (a • x) • x ? 17
Jean-Michel Muller (CNRS, LIP, University de Lyon, France)

Analyzing the Impact of Floating-Point Precision Adaptation in Iterative Programs 25
Guillaume Revy (Univ Perpignan Via Domitia/LIRMM, Perpignan, France)

Shadow Computation with BFloat16 to Estimate the Numerical Accuracy of Summations 33
David Defour (LAMPS, Univ. of Perpignan via Domitia, France), Pablo de Oliveira Castro (Université Paris-Saclay, UVSQ, LI-PaRAD, ECR, France), Matei Istoan (Université Paris-Saclay, UVSQ, LI-PaRAD, ECR, France), and Eric Petit (Intel Corp.)

Session 3: Arithmetic operators (1)

Pipeline Optimization using a Cost Extension of Timed Petri Nets 37
Rémi Parrot (École Centrale de Nantes, LS2N, France), Mikaël Briday (École Centrale de Nantes, LS2N, France), and Olivier H. Roux (École Centrale de Nantes, LS2N, France)

Approximate Floating-Point Operations with Integer Units by Processing in the Logarithmic Domain 45
Oscar Gustafsson (Linköping University, Sweden) and Noah Hellman (Linköping University, Sweden)

XpulpNN: Enabling Energy Efficient and Flexible Inference of Quantized Neural Networks on RISC-V based IoT End Nodes 53
Angelo Garofalo (Universita degli Studi di Bologna Scuola di Ingegneria e Architettura), Giuseppe Tagliavini (Universita degli Studi di Bologna Scuola di Ingegneria e Architettura), Francesco Conti (University of Bologna), Luca Benini (University of Bologna), and Davide Rossi (University of Bologna)

Session 4: Custom precision floating point mathematical libraries

Acceleration of LU Decomposition Supporting Double-Double, Triple-Double, and Quadruple-Double Precision Floating-Point Arithmetic with AVX2 54
Tomonori Kouya (Shizuoka Institute of Science and Technology, Japan)

A Study of the Effects and Benefits of Custom-Precision Mathematical Libraries for HPC Codes 62
Emeric Brun (CEA-Marcoule, French Alternative Energies and Atomic Energy Commission), David Defour (Perpignan University), Pablo De Oliveira Castro (Université de Versailles Saint-Quentin en Yvelines UFR des Sciences), Matei Istoan (Versailles Saint-Quentin-en-Yvelines University), Davide Mancusi (CEA-Saclay, French Alternative Energies and Atomic Energy Commission), Eric Petit (Math Library Pathfinding Group, Intel Corp), and Alan Vaquet (Versailles Saint-Quentin-en-Yvelines University)

Manifest for an Approximation Exchange Format 63
Nicolas Brunie (Kalray)

Session 5: Stochastic computing

Algorithms for Stochastically Rounded Elementary Arithmetic Operations in IEEE 754 Floating-Point Arithmetic 69
Massimiliano Fasi (The University of Manchester) and Mantas Mikaitis (The University of Manchester)

Dither Computing: A Hybrid Deterministic-Stochastic Computing Framework 70
Chai Wah Wu (IBM T. J. Watson Research Center, USA)

Session 6: Arithmetic for Cryptography (1)

MPHELL: A Fast and Robust Library with Unified and Versatile Arithmetics for Elliptic Curves Cryptography 78
Titouan Coladon (Université Grenoble Alpes, France), Philippe Elbaz-Vincent (Université Grenoble Alpes, France), and Cyril Hugounenq (Université Grenoble Alpes, France)

Generating Residue Number System Bases 86
Jean-Claude Bajard (Sorbonne Universite, CNRS, INRIA, Institut de Mathematiques de Jussieu-Paris Rive Gauche, France), Kazuhide Fukushima (Information Security Laboratory of KDDI Research, Inc, Japan), Shinsaku Kiyomoto (Information Security Laboratory of KDDI Research, Inc, Japan), Thomas Plantard (Institute of Cybersecurity and Cryptology, University of Wollongong, Australia), Arnaud Sipasseuth (Information Security Laboratory of KDDI Research, Inc, Japan), and Willy Susilo (Institute of Cybersecurity and Cryptology, University of Wollongong, Australia)

High-Speed NTT-Based Polynomial Multiplication Accelerator for Post-Quantum Cryptography 94
Mojtaba Bisheh-Niasar (Florida Atlantic University), Reza Azarderakhsh (Florida Atlantic University), and Mehran Mozaffari-Kermani (Florida Atlantic University)

Session 7: Arithmetic operators (2)

Resource Optimal Truncated Multipliers for FPGAs 102
Andreas Böttcher (Fulda, University of Applied Science, Germany), Martin Kumm (Fulda, University of Applied Science, Germany), and Florent de Dinechin (Univ Lyon, INSA Lyon, Inria, CITI, Lyon, France)

Sum Propagate Adders 110
Giorgos Dimitrakopoulos (Democritus University of Thrace), Kleanthis Papachatzopoulos (University of Patras), and Vassilis Paliouras (University of Patras)

Session 8: Special Session on "Hardware and Software Tools for Computer Arithmetic"

Some Formal Tools for Computer Arithmetic: Flocq and Gappa 111
Sylvie Boldo (Université Paris-Saclay, CNRS, ENS Paris-Saclay, Inria, Laboratoire Méthodes Formelles, France) and Guillaume Melquiond (Université Paris-Saclay, CNRS, ENS Paris-Saclay, Inria, Laboratoire Méthodes Formelles, France)

Towards Arithmetic-Centered Filter Design 115
Florent de Dinechin (INSA Lyon, France), Silviu-Ioan Filip (Univ Rennes, Inria, CNRS, IRISA, France), Martin Kumm (Fulda University of Applied Science, Germany), and Anastasia Volkova (Université de Nantes, France)

FPGA Acceleration of Bit-True Simulations for Word-Length Optimization 119
Javier Hormigo (Universidad de Málaga, Spain) and Gabriel Caffarena (University CEU-San Pablo, Spain)

Session 9: Arithmetic for Cryptography (2)

A Faster Hardware Implementation of the AES S-box 123
Doaa Ashmawy (Western University, Canada) and Arash Reyhani-Masoleh (Western University, Canada)

Accelerated RISC-V for SIKE 131
Rami Elkhatib (Florida Atlantic University), Reza Azarderakhsh (Florida Atlantic University), and Mehran Mozaffari-Kermani (University of South Florida)

Efficient Word Size Modular Arithmetic 139
Thomas Plantard (University of Wollongong)

Author Index 141