ARITH-26 (2019) Program

Monday, June 10

9:00- 9:15 Opening

9:15-10:15 Keynote 1

Error Bounds for Computer Arithmetics

Siegfried M. Rump (Hamburg University of Technology, Germany)

10:15-10:35 Coffee Break

10:35-12:15 Session 1: Numerical Computation and Floating-Point Arithmetic

Faster Arbitrary-Precision Dot Product and Matrix Multiplication

Fredrik Johansson (LFANT - Inria Bordeaux, France)

Accurate Complex Multiplication in Floating-Point Arithmetic

Vincent Lefèvre (Univ Lyon, EnsL, UCBL, CRS, Inria, LIP, France) and
Jean-Michel Muller (Univ Lyon, EnsL, UCBL, CRS, Inria, LIP, France)

Exchange Algorithm for Evaluation and Approximation Error-Optimized Polynomials

Denis Arzelier (LAAS-CNRS, Univ de Toulouse, France),
Florent Bréhard (ENS de Lyon, LAAS-CNRS, France) and
Mioara Joldes (LAAS-CNRS, Univ de Toulouse, France)

Reproducible Summation Under HUB Format

Julio Villalba-Moreno (University of Málaga, Spain),
Javier Hormigo (University of Málaga, Spain) and
Francisco Jaime (University of Málaga, Spain)

12:15-13:30 Lunch

13:30-14:20 Session 2: Arithmetic for Cryptography 1

Hierarchical Approach in RNS Base Extension for Asymmetric Cryptography

Libey Djath (Université de Bretagne Occidentale, France),
Karim Bigou (Université de Bretagne Occidentale, France) and
Arnaud Tisserand (CNRS, France)

Efficient Implementation of Modular Division by Input Bit Splitting

Danila Gorodecky (National Academy of Science of Belarus, Belarus) and
Tiziano Villa (Verona University, Italy)

14:20-14:30 Short Break

14:30-15:45 Session 3: Arithmetic for Machine Learning and Graphics

Scalar Arithmetic Multiple Data: Customizable Precision for Deep Neural Networks

Andrew Anderson (Trinity College Dublin, Ireland),
Michael J. Doyle (Trinity College Dublin, Ireland) and
David Gregg (Trinity College Dublin, Ireland)

Leveraging the bfloat16 Artificial Intelligence Datatype for Higher-Precision Computations

Greg Henry (Intel Corporation, USA),
Ping Tak Peter Tang (Intel Corporation, USA) and
Alexander Heinecke (Intel Corporation, USA)

New 3D Projection Transformation for Point Clouds

Alvaro Vazquez (University of Santiago de Compostela, Spain) and
Elisardo Antelo (University of Santiago de Compostela, Spain)

15:45-16:10 Coffee Break

16:10-18:15 Session 4: Special Session - Industrial Arithmetic (Coordinator: Elisardo Antelo)

Optimized Fused Floating-Point Many-Term Dot-Product Hardware for Machine Learning Accelerators

Himanshu Kaul (Intel Corporation, USA),
Mark Anders (Intel Corporation, USA),
Sanu Mathew (Intel Corporation, USA),
Seongjong Kim (Intel Corporation, USA) and
Ram Krishnamurthy (Intel Corporation, USA)

Bfloat16 processing for Neural Networks

Neil Burgess (Arm, UK),
Nigel Stephens (Arm, UK),
Jelena Milanovic (Arm, France),
Konstantinos Monachopoulos (Arm, UK) and
David Mansell (Arm, UK)

DLFloat: A 16-bit Floating Point Format Designed for Deep Learning Training and Inference

Ankur Agrawal (IBM, USA),
Silvia M. Mueller (IBM, Germany),
Bruce M. Fleischer (IBM, USA),
Jungwook Choi (IBM, USA),
Naigang Wang (IBM, USA),
Xiao Sun (IBM, USA) and
Kailash Gopalakrishnan (IBM, USA)

New Technologies for Improved Computing

Marius Cornea (Intel Corporation, USA)

ARM Floating Point 2019: Latency, Area, Power

David R. Lutz (ARM Austin Design Center, USA)

Tuesday, June 11

8:40- 9:40 Keynote 2

Big Numbers for a Big Universe

Andrew Ensor (Auckland University of Technology, New Zealand)

9:40- 9:45 Short Break

9:45-10:55 Session 5: Short Papers and Student Session

Precise and Concise Graphical Representation of the Natural Numbers

David Matula (Southern Methodist University, USA)
and Zizhen Chen (Southern Methodist Univ., USA)

Dynamic Precision Numerics Using a Variable-Precision UNUM type I HW Coprocessor

Andrea Bocco (Univ. Grenoble Alpes, CEA-LETI, France),
Yves Durand (Univ. Grenoble Alpes, CEA-LETI,France) and

Florent De Dinechin (INSA-Lyon, France)

A Cost-Efficient Iterative Truncated Logarithmic Multiplication for Convolutional Neural Networks

HyunJin Kim (Dankook University, South Korea),
Min Soo Kim (University of California, Irvine, USA),
Alberto A. Del Barrio (Universidad Complutense de Madrid, Spain) and
Nader Bagherzadeh (University of California, Irvine, USA)

Under- and Overflow Detection in the Residue Logarithmic Number System

Mark Arnold (XLNS Research, USA),
Ioannis Kouretas (University of Patras, Greece),
Vassilis Paliouras (University of Patras, Greece) and
John Cowles (University of Wyoming, USA)

Experimental Analysis of Matrix Multiplication Functional Units

Brian Hickmann (Intel Corporation, USA) and
Dennis Bradford (Intel Corporation, USA)

Performance Evaluation of an Efficient Double-Double BLAS1 Function With Error-Free Transformation and its Application to Explicit Extrapolation Methods

Tomonori Kouya (Shizuoka Institute of Science and Technology, Japan)

<Invited Student Presentation>

A Perspective into Squarer Optimization

Katherine Parry (Central High Scool, Rapid City, South Dakota, USA)

10:55-11:15 Coffee Break (Poster Discussion for the short papers)

11:15-12:55 Session 6: Adders and Multipliers

An Ultra-Fast Parallel Prefix Adder

Kumar Sambhav Pandey (National Institute of Technology, Hamipur and Indian Institute of Technology, India),
Dinesh Kumar B (Indian Institute of Technology, Mandi, India),
Neeraj Goel (Indian Institute of Technology, Ropar, India) and
Hitesh Shrimali (Indian Institute of Technology, Mandi, India)

Modulo-(2^n+3) Parallel Prefix Addition via Diminished-3 Representation of Residues

Ghassem Jaberipur (Shahid Beheshti University, Iran) and
Sahar Moradi Cherati (Shahid Beheshti University, Iran)

High-Throughput Multiplier Architectures Enabled by Intra-Unit Fast Forwarding

Jihee Seo (Washington State University, USA) and
Dae Hyun Kim (Washington State Univ., USA)

Table-Based versus Shift-And-Add Constant Multipliers for FPGAs

Florent de Dinechin (Univ Lyon, INSA Lyon, Inria, CITI, France),
Silviu-Ioan Filip (Univ Renees, Inria, CNRS, IRISA, France),
Luc Forget (Univ Lyon, INSA Lyon, Inria, CITI, France) and
Martin Kumm (University of Applied Science, Germany)

12:55-14:25 Lunch

(13:55-14:25 Poster Discussion for the short papers)

14:25-16:05 Session 7: Error Analysis and Verification

Optimal Bounds for Floating-Point Addition in Constant Time

Mak Andrlon (University of Melbourne, Australia),
Peter Schachte (University of Melbourne, Australia),
Harald Søndergaard (University of Melbourne, Australia) and
Peter J. Stuckey (Monash University, Australia)

Semi-Automatic Implementation of the Complementary Error Function

Anastasia Volkova (Univ Lyon, Inria, CNRS, ENS de Lyon, Université Claude Bernard Lyon 1, France) and
Jean-Michel Muller (Univ Lyon, CNRS, ENS de Lyon, Inria, Université Claude Bernard Lyon 1, France)

Optimal Word-Length Allocation for the Fixed-Point Implementation of Linear Filters and Controllers

Thibault Hilaire (Sorbonne Université, INRIA, Université Paris-Saclay, France),
Hacène Ouzia (Sorbonne Université , France) and
Benoit Lopez

Formal Verification of a State-of-the-Art Integer Square Root

Guillaume Melquiond (Inria, Université Paris-Saclay, France) and
Raphaël Rieu-Helft (TrustInSoft, Inria, Université Paris-Saclay, France)

16:05-16:30 Coffee Break

16:30-18:10 Session 8: Special Session - Automatic Datapath Generators (Coordinator: Florent de Dinechin)

Reflections of 10 Years of FloPoCo

Florent de Dinechin (Univ Lyon, INSA Lyon, France)

DSL-Based Modular IP Core Generators: Example FFT and Related Structures

François Serre (ETH Zurich, Switzerland) and
Markus Püschel (ETH Zurich, Switzerland)

Compile-Time Generation of Custom-Precision Floating-Point IP using HLS Tools

David B. Thomas (Imperial College London, UK)

Hybrid Dot-Product Design for FP-Enabled FPGAs

Bogdan Pasca (Intel Corporation, France)

18:30-20:30 Banquet

Wednesday, June 12

8:40-10:30 Keynote 3

Computer Arithmetic Research to Accelerate Privacy-Protecting Encrypted Computing Such as Homomorphic Encryption

Kurt Rohloff (New Jersey Institute of Technology, USA)

Privacy-Preserving Deep Learning via Additively Homomorphic Encryption

Shiho Moriai (National Institute of Information and Communications Technology, Japan)

10:30-10:50 Coffee Break

10:50-12:05 Session 9: Arithmetic for Cryptography 2

Randomization of Arithmetic Over Polynomial Modular Number System

Laurent-Stéphane Didier (Université de Toulon, France),
Fangan Yssouf Dosso (Université de Toulon, France),

Nadia El Mrabet (Ecole des Mines de St Etienne, France),
Jérémy Marrez (Sorbonne Université, France) and
Pascal Véron (Université de Toulon, France)

HyPoRes: An Hybrid Representation System for ECC

Paulo Martins (INESC-ID, Instituto Superior Técnico, Universidate de Lisboa, Portugal),
Jérémy Marrez (Sorbonne Université, CNRS, France),
Jean Claude Bajard (Sorbonne Université, CNRS, France) and
Leonel Sousa (INESC-ID, Instituto Superior Téchnico, Universidate de Lisboa, Portugal)

Using the New VPMADD Instructions for the New Post Quantum Key Encapsulation Mechanism SIKE

Shay Gueron (University of Haifa, Israel, Amazon USA) and
Dusan Kostic (École Polytechnique Fédérale de Lausanne, Switzerland)

12:05-12:15 Closing

Lunch (Lunch Box)