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 (INRIA, France)

Accurate Complex Multiplication in Floating-Point Arithmetic

Vincent Lefevre (INRIA, France) and Jean-Michel Muller (CNRS, France)

Exchange algorithm for evaluation and approximation error-optimized polynomials

Denis Arzelier (LAAS-CNRS, France), Florent Brehard (ENS Lyon, France)
and Mioara Joldes (CNRS, France)

Reproducible Summation under HUB Format

Julio Villalba-Moreno, Javier Hormigo and Francisco Jaime Rodriguez (Univ. Malaga, 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 Okonfu Djath, Karim Bigou (Univ. Bretagne Occidentale, France)
and Arnaud Tisserand (CNRS, France)

Efficient Implementation of Modular Division by Input Bit Splitting

Danila Gorodecky (NAS, Belarus) and Tiziano Villa (Univ. Verona, 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, Michael Doyle and David Gregg (Trinity College Dublin, Ireland)

Leveraging the bfloat16 Artificial Intelligence Datatype for Higher-Precision Computations

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

New 3D Projection Transformation for Point Clouds

Alvaro Vazquez and Elisardo Antelo (Univ. 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, Mark Anders, Sanu Mathew, Seongjong Kim and Ram Krishnamurthy
(Intel, USA)

Bfloat16 processing for Neural Networks

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

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

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

New Technologies for Improved Computing

Marius Cornea (Intel, USA)

ARM Floating Point 2019: Latency, Area, Power

David Lutz (ARM, UK)

Tuesday, June 11

8:40- 9:40 Keynote 2

Big numbers for a big universe

Andrew Ensor (SKA, 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 and Zizhen Chen (Southern Methodist Univ., USA)

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

Andrea Bocco (Univ. Grenoble Alpes, France), Yves Durand (Univ. Grenoble Alpes, France) and Florent De Dinechin (INSA-Lyon, France)

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

Hyun Jin Kim (Dankook Univ., South Korea), Min Soo Kim (U.C. Irvine, USA), Alberto A. Del Barrio (Complutense Univ. of Madrid, Spain) and Nader Bagherzadeh (U.C. Irvine, USA)

Under- and Overflow Detection in the Residue Logarithmic Number System

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

Experimental Analysis of Matrix Multiplication Functional Units

Brian Hickmann and Dennis Bradford (Intel, 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 (South Dakota School of Mines and Technology, 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, Dinesh Kumar B, Neeraj Goel (IIT Ropar, India) and Hitesh Shrimali (IIT Mandi, India)

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

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

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

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

Table-Based versus Shift-And-Add Constant Multipliers for FPGAs
Florent de Dinechin (INSA Lyon, Francs), Silviu Filip (INRIA, France),
Luc Forget (INSA Lyon, Francs) and Martin Kumm (Univ. Applied Sciences, Fulda, Germany)

12:55-14:25 Lunch, SC meeting

(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, Peter Schachte, Harald Sondergaard (Univ. Melbourne, Australia)
and Peter J. Stuckey (Monash Univ., Australia)

Semi-automatic implementation of the complementary error function
Anastasia Volkova and Jean-Michel Muller (Univ. Lyon, France)

Optimal word-length allocation for the fixed-point implementation of linear filters and controllers
Thibault Hilaire, Hacene Ouzia (Sorbonne Univ., France) and Benoit Lopez

Formal verification of a state-of-the-art integer square root
Guillaume Melquiond (INRIA, France) and Raphael Rieu-Helft (TrustInSoft/Inria, 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 (INSA, France)

DSL-based modular IP core generators: Example FFT and related structures
Francois Serre and Markus Pueschel (ETHZ, Switzerland)

Compile-time generation of custom-precision floating-point IP using HLS tools
David Thomas (Imperial College, UK)

Hybrid dot-product design for FP-enabled FPGAs
Bogdan Pasca (Intel, France)

18:30- Banquet

Wednesday, June 12

8:40-10:30 Keynote 3

Computer Arithmetic Research to Accelerate Privacy-Protecting Encrypted Computing
such as Homomorphic Encryption
Kurt R. 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-Stephane Didier, Fangan Yssouf Dosso (Univ. Toulon, France),
Nadia El Mrabet(SAS-CGCP, France), Jeremy Marrez (CNRS, France)
and Pascal Veron (Univ. Toulon, France)

HyPoRes: An Hybrid Representation System for ECC
Paulo Martins (INESC-ID, Portugal), Jeremy Marrez (LIP6-UPMC, France)

Jean Claude Bajard (LIP6-UPMC, France) and Leonel Sousa (INESC-ID, Portugal)

Using the new VPMADD instructions for the new post quantum key encapsulation mechanism SIKE

Shay Gueron (Univ. Haifa / AWS, Israel) and Dusan Kostic (EPF Lausanne, Switzerland)

12:05-12:15 Closing

Lunch (Lunch Box)