

23rd IEEE Symposium on Computer Arithmetic

ARITH 23

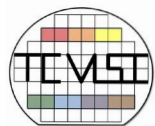


Santa Clara, California, 10-13 July 2016

Editors: Paolo Montuschi, Michael Schulte, Javier Hormigo, Stuart Oberman, and Nathalie Revol



IEEE  computer society
CELEBRATING 70 YEARS



Technical Committee
on
VLSI

SYNOPSYS[®]
Accelerating Innovation



CONFERENCE INFORMATION

PAPERS BY SESSION

PAPERS BY AUTHOR

GETTING STARTED

TRADEMARKS

SEARCH

Conference Information

2016 IEEE 23rd Symposium on Computer Arithmetic

- Foreword
- Committees
- Reviewers
- Keynote Talks and Special Sessions
- Title Page (Book version)
- Copyright Page (Book version)
- Table of Contents (Book version)
- Author Index (Book version)
- Publisher's Information (Book version)

Sessions

- Session 1: Arithmetic Units
- Session 2: Security and Cryptography (I)
- Session 3: Big Numbers
- Session 4: Accuracy and Reproducibility
- Session 5: Floating-Point Implementations
- Session 6: Less-conventional Number Systems (I)
- Session 7: Security and Cryptography (II)
- Session 8: Less-conventional Number Systems (II)
- Session 9: Logarithm Implementations

Papers by Session

Session 1: Arithmetic Units

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

Papers by Session

Session 2: Security and Cryptography (I)

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

Papers by Session

Session 3: Big Numbers

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

Papers by Session

Session 4: Accuracy and Reproducibility

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

Papers by Session

Session 5: Floating-Point Implementations

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

Papers by Session

Session 6: Less-conventional Number Systems (I)

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

Papers by Session

Session 7: Security and Cryptography (II)

- ❑ Hardware Implementation of AES Using Area-Optimal Polynomials for Composite-Field Representation $GF(24)^2$ of $GF(28)$
Shay Gueron and Sanu Mathew
- ❑ Random Digit Representation of Integers
Nicolas Méloni and M. Anwar Hasan
- ❑ Hybrid Position-Residues Number System
Karim Bigou and Arnaud Tisserand

Papers by Session

Session 8: Less-conventional Number Systems (II)

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

Papers by Session

Session 9: Logarithm Implementations

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

Papers by Author

A

- Abedi, Dariush
- Ahmed, Syed Ershad

B

- Bajard, Jean-Claude
- Bayram, Anil
- Benini, Luca
- Bigou, Karim
- Brunie, Nicolas
- Brzicová, Marta

C

- Carlough, Steven
- Cui, Xiaoping

d

- de Dinechin, Florent
- de Oliveira Castro, Pablo

D

- Denis, Christophe

E

- Emmart, Niall
- Eynard, Julien

F

- Frougny, Christiane

G

- Gautschi, Michael

Papers by Author

- Geran, Amir Ali Kouzeh
- Gören, Sezer
- Gueron, Shay
- Gürkaynak, Frank K.

H

- Hasan, M. Anwar

J

- Jaberipur, Ghassem

K

- Kadam, Sanket
- Krasnov, Vlad

L

- Langhammer, Martin

- Langlois, Philippe
- Le Maire, Julien
- Lecerf, Grégoire
- Lefèvre, Vincent
- Levent, Vecdi Emre
- Lichtenau, Cedric
- Liu, Weiqiang
- Lombardi, Fabrizio
- Luitjens, Justin

M

- Mathew, Sanu
- Méloni, Nicolas
- Merkiche, Nabil
- Mueller, Silvia Melitta
- Muller, Jean-Michel

Papers by Author

N

- Nheili, Rafife

P

- Parhami, Behrooz
- Pasca, Bogdan
- Pelantová, Edita
- Petit, Eric
- Popescu, Valentina

R

- Revy, Guillaume
- Reyhani-Masoleh, Arash

S

- Schaffner, Michael

- Srinivas, M. B.
- Svobodová, Milena

T

- Tang, Ping Tak Peter
- Tisserand, Arnaud

U

- Ugurdag, H. Fatih

V

- van der Hoeven, Joris

V

- Villalba-Moreno, Julio

Papers by Author

W

- Weems, Charles
- Wenwen, Dong
- Woolley, Cliff

Papers by Author

Abedi, Dariush

- ❑ A Formulation of Fast Carry Chains Suitable for Efficient Implementation with Majority Elements

Ahmed, Syed Ershad

- ❑ An Iterative Logarithmic Multiplier with Improved Precision

Bajard, Jean-Claude

- ❑ Multi-fault Attack Detection for RNS Cryptographic Architecture

Bayram, Anil

- ❑ Efficient Combinational Circuits for Division by Small Integer Constants

Benini, Luca

- ❑ Accuracy and Performance Trade-Offs of Logarithmic Number Units in Multi-Core Clusters

Papers by Author

Bigou, Karim

- Hybrid Position-Residues Number System

Brunie, Nicolas

- Computing floating-point logarithms with fixed-point operations

Brzicová, Marta

- On-line Multiplication and Division in Real and Complex Bases

Carlough, Steven

- Quad Precision Floating Point on the IBM z13™

Cui, Xiaoping

- A Parallel Decimal Multiplier Using Hybrid Binary Coded Decimal (BCD) Codes

Papers by Author

de Dinechin, Florent

- Computing floating-point logarithms with fixed-point operations

de Oliveira Castro, Pablo

- Verificarlo: Checking Floating Point Accuracy through Monte Carlo Arithmetic

Denis, Christophe

- Verificarlo: Checking Floating Point Accuracy through Monte Carlo Arithmetic
- Recovering Numerical Reproducibility in Hydrodynamic Simulations

Emmart, Niall

- Optimizing Modular Multiplication for NVIDIA's Maxwell GPUs

Eynard, Julien

- Multi-fault Attack Detection for RNS Cryptographic Architecture

Papers by Author

Frougny, Christiane

- ❑ On-line Multiplication and Division in Real and Complex Bases

Gautschi, Michael

- ❑ Accuracy and Performance Trade-Offs of Logarithmic Number Units in Multi-Core Clusters

Geran, Amir Ali Kouzeh

- ❑ A CRC-Based Concurrent Fault Detection Architecture for Galois/Counter Mode (GCM)

Gören, Sezer

- ❑ Efficient Combinational Circuits for Division by Small Integer Constants

Gueron, Shay

- ❑ Accelerating Big Integer Arithmetic Using Intel IFMA Extensions

Papers by Author

- ❑ Hardware Implementation of AES Using Area-Optimal Polynomials for Composite-Field Representation $GF(24)_2$ of $GF(28)$

Gürkaynak, Frank K.

- ❑ Accuracy and Performance Trade-Offs of Logarithmic Number Units in Multi-Core Clusters

Hasan, M. Anwar

- ❑ Random Digit Representation of Integers

Jaberipur, Ghassem

- ❑ A Formulation of Fast Carry Chains Suitable for Efficient Implementation with Majority Elements

Kadam, Sanket

- ❑ An Iterative Logarithmic Multiplier with Improved Precision

Papers by Author

Krasnov, Vlad

- ❑ Accelerating Big Integer Arithmetic Using Intel IFMA Extensions

Langhammer, Martin

- ❑ Single Precision Natural Logarithm Architecture for Hard Floating-Point and DSP-Enabled FPGAs

Langlois, Philippe

- ❑ Recovering Numerical Reproducibility in Hydrodynamic Simulations

Le Maire, Julien

- ❑ Computing floating-point logarithms with fixed-point operations

Lecerf, Grégoire

- ❑ Evaluating Straight-Line Programs over Balls

Papers by Author

Lefèvre, Vincent

- Correctly Rounded Arbitrary-Precision Floating-Point Summation

Levent, Vecdi Emre

- Efficient Combinational Circuits for Division by Small Integer Constants

Lichtenau, Cedric

- Quad Precision Floating Point on the IBM z13™

Liu, Weiqiang

- A Parallel Decimal Multiplier Using Hybrid Binary Coded Decimal (BCD) Codes

Lombardi, Fabrizio

- A Parallel Decimal Multiplier Using Hybrid Binary Coded Decimal (BCD) Codes

Papers by Author

Luitjens, Justin

- ❑ Optimizing Modular Multiplication for NVIDIA's Maxwell GPUs

Mathew, Sanu

- ❑ Hardware Implementation of AES Using Area-Optimal Polynomials for Composite-Field Representation $GF(24)^2$ of $GF(28)$

Méloni, Nicolas

- ❑ Random Digit Representation of Integers

Merkiche, Nabil

- ❑ Multi-fault Attack Detection for RNS Cryptographic Architecture

Mueller, Silvia Melitta

- ❑ Quad Precision Floating Point on the IBM z13™

Papers by Author

Muller, Jean-Michel

- ❑ A New Multiplication Algorithm for Extended Precision Using Floating-Point Expansions
- ❑ Computing floating-point logarithms with fixed-point operations

Nheili, Rafife

- ❑ Recovering Numerical Reproducibility in Hydrodynamic Simulations

Parhami, Behrooz

- ❑ A Formulation of Fast Carry Chains Suitable for Efficient Implementation with Majority Elements

Pasca, Bogdan

- ❑ Single Precision Natural Logarithm Architecture for Hard Floating-Point and DSP-Enabled FPGAs

Papers by Author

Pelantová, Edita

- ❑ On-line Multiplication and Division in Real and Complex Bases

Petit, Eric

- ❑ Verificarlo: Checking Floating Point Accuracy through Monte Carlo Arithmetic

Popescu, Valentina

- ❑ A New Multiplication Algorithm for Extended Precision Using Floating-Point Expansions

Revy, Guillaume

- ❑ Automated Design of Floating-Point Logarithm Functions on Integer Processors

Reyhani-Masoleh, Arash

- ❑ A CRC-Based Concurrent Fault Detection Architecture for Galois/Counter Mode (GCM)

Papers by Author

Schaffner, Michael

- Accuracy and Performance Trade-Offs of Logarithmic Number Units in Multi-Core Clusters

Srinivas, M. B.

- An Iterative Logarithmic Multiplier with Improved Precision

Svobodová, Milena

- On-line Multiplication and Division in Real and Complex Bases

Tang, Ping Tak Peter

- A New Multiplication Algorithm for Extended Precision Using Floating-Point Expansions

Tisserand, Arnaud

- Hybrid Position-Residues Number System

Papers by Author

Ugurdag, H. Fatih

- Efficient Combinational Circuits for Division by Small Integer Constants

van der Hoeven, Joris

- Evaluating Straight-Line Programs over Balls

Villalba-Moreno, Julio

- Digit Recurrence Floating-Point Division under HUB Format

Weems, Charles

- Optimizing Modular Multiplication for NVIDIA's Maxwell GPUs

Wenwen, Dong

- A Parallel Decimal Multiplier Using Hybrid Binary Coded Decimal (BCD) Codes

Papers by Author

Woolley, Cliff

- ❑ Optimizing Modular Multiplication for NVIDIA's Maxwell GPUs

Papers by Author

A	B	C	D	E	F	G
H	I	J	K	L	M	N
O	P	Q	R	S	T	U
V	W	X	Y	Z		