Proceedings

18th IEEE Symposium on Computer Arithmetic

Montpellier, France

June 25-27, 2007

Los Alamitos, California

Washington • Tokyo

Table of Contents

18th IEEE Symposium on Computer Arithmetic (ARITH-18 2007)

Foreword ix
Program Committee x
Steering Committee / Symposium Committee xi
Reviewers xii

Session 1: Keynote Talk
Chair: Graham Jullien

The Return of Silicon Efficiency 3
Simon Knowles

Session 2: Basic Arithmetic Operations I
Chair: Luigi Dadda

Serial Parallel Multiplier Design in Quantum-dot Cellular Automata 7
Heumpil Cho and Earl Swartzlander

Robust Energy-Efficient Adder Topologies 16
Dinesh Patil, Omid Azizi, Ron Ho, Mark Horowitz, and Rajesh Ananthraman

Session 3: Decimal Floating Point
Chair: Neil Burgess

A Software Implementation of the IEEE 754R Decimal Floating-Point Arithmetic Using the Binary Encoding Format 29
Marius Cornea, Cristina Anderson, John Harrison, Ping Tak Peter Tang, Eric Schneider, and Charles Tsen

Solving Constraints on the Intermediate Result of Decimal Floating-Point Operations 38
Merav Aharoni, Ron Maharik, and Abraham Ziv

Decimal Floating-Point Multiplication via Carry-Save Addition 46
Mark Erle, Mike Schulte, and Brian Hickman

Decimal Floating-Point Adder and Multifunction Unit with Injection-Based Rounding 56
Liang-Kai Wang and Mike Schulte

Session 4: Floating Point Implementation
Chair: John Harrison

A New Architecture for Multiple-precision Floating-point Multiply-add Fused Unit Design 69
Libo Huang, Li Shen, Kui Dai, and Zhiyang Wang

P6 Binary Floating-Point Unit 77
Eric Schwarz, Son Dao Trong, Martin Schmookler, and Michael Kroener

Design of the ARM VFP11 Divide and Square Root Synthesisable Macrocell 87
Neil Burgess and Christopher Hinds

Session 5: Crypto Algorithms

Chair: Jean-Claude Bajard

An Algorithm for the η_T Pairing Calculation in Characteristic Three and its Hardware Implementation 97
Jean-Luc Beuchat, Masaaki Shirase, Tsuyoshi Takagi, and Eiji Okamoto

An Algorithm for Inversion in GF(2^m) Suitable for Implementation Using a Polynomial Multiply Instruction on GF(2) 105
Katsuki Kobayashi, Naofumi Takagi, and Kazuyoshi Takagi

Asymmetric Squaring Formulae 113
Jaewook Chung and M. Anwar Hasan

Spectral Modular Exponentiation 123
Gökay Saldamlı and Çetin Koç

Session 6: Various Topics

Chair: Israel Koren

Worst Cases of a Periodic Function with Large Arguments 133
Guillaume Hanrot, Vincent Lefèvre, Damien Stehlé, and Paul Zimmermann

How to Ensure a Faithful Polynomial Evaluation with the Compensated Horner Algorithm 141
Philippe Langlois and Nicolas Louvet

Accurate Multiple-Precision Gauss-Legendre Quadrature 150
Laurent Fousse

Session 7: Elementary Functions

Chair: Elisardo Antelo

Return of the Hardware Floating-Point Elementary Function 161
Jérémie Detrey, Florent de Dinechin, and Xavier Pujol

Efficient Polynomial L^∞-Approximations 169
Nicolas Brisebarre and Sylvain Chevillard

Floating-Point L^2-Approximations to Functions 177
Nicolas Brisebarre and Guillaume Hanrot

Session 8: Floating Point Issues and Operations

Chair: Eric Schwarz

Formal Verification of Floating-Point Programs 187
Jean-Christophe Filliâtre and Sylvie Boldo

A New Family of High-Performance Parallel Decimal Multipliers 195
Alvaro Vázquez, Elisardo Antelo, and Paolo Montuschi

Optimistic Parallelization of Floating-Point Accumulation 205
Nachiket Kapre and André DeHon

Session 9: Modular Operations

Chair: Naofumi Takagi

Modular Multiplication Using Redundant Digit Division 217
Ping Tak Peter Tang

Fast Modular Reduction 225
William Hasenplaugh, Vinodh Gopal, and Gunnar Gaubatz

Montgomery Reduction Algorithm for Modular Multiplication Using
Low-Weight Polynomial Form Integers 230
Jaewook Chung and M. Anwar Hasan

Efficient Method for Magnitude Comparison in RNS Based on Two Pairs of Conjugate Moduli 240
Leonel Sousa

Session 10: Basic Arithmetic Operations II

Chair: Tomas Lang

Performing Advanced Bit Manipulations Efficiently in General-Purpose Processors 251
Yedidya Hilewitz and Ruby B. Lee

Multiplication by a Constant is Sublinear 261
Vassil Dimitrov, Laurent Imbert, and Andrew Zakaluzny

Author Index **269**