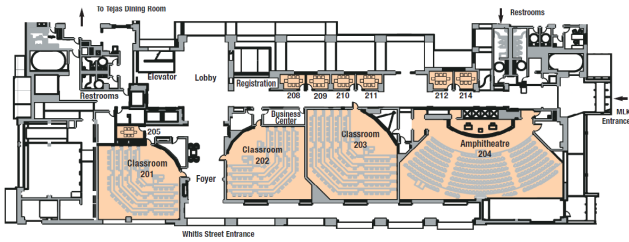


The Symposium sessions are held in the AT&T Conference Center Amphitheatre (204). Lunches and coffee breaks will be in the Center's restaurant.



Symposium Banquet

The Banquet will be held on Tuesday April 9th at

Abel's on the Lake
3825 Lake Austin Blvd
Austin, TX 78703



Free busses will leave the Conference Center at 6.30 pm.

Wednesday Afternoon Excursion

After the conference, we propose a coach tour of the central Texas Hill Country, including visits to the very popular [Lady Bird Johnson Wildflower Center](#) and to the [Lyndon B. Johnson National Historical Park](#) in Johnson City, where the following attractions are located:

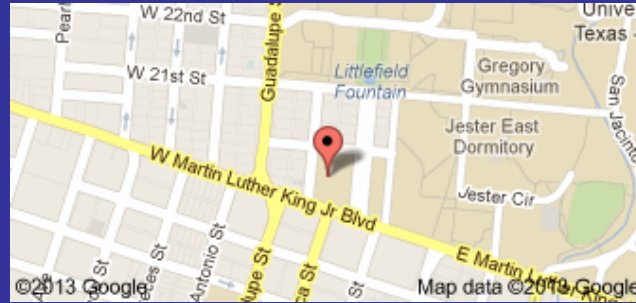
- The National Park Visitor Center
- The Boyhood Home
- The Johnson Settlement



More info at: <http://arithsymposium.org/social.html>

CONFERENCE VENUE

AT&T Executive Education Conference Center
1900 University Avenue
Austin, Texas 78705
512-404-1900



Parking

Overnight car parking at UT AT&T center is \$16.00 per night, and daytime only parking is \$8.00 (one-time use voucher) or \$9.00 (in/out voucher).

Car park charges are not included in the conference fee.

ARITH-21 ORGANIZING COMMITTEE

General Chairs

Neil Burgess, ARM, USA
David W. Matula, Southern Methodist University, USA

Program Chairs

Alberto Nannarelli, Technical University, Denmark
Peter-Michael Seidel, University of Hawaii, USA
Ping Tak Peter Tang, Intel, USA

Financial Chair

Michael Schulte, AMD, USA

Local Arrangements Chair

Kevin Nowka, IBM, USA

21st IEEE Symposium on
Computer Arithmetic

ARITH 21



April 7-10, 2013

AT&T Conference Center, Austin, Texas, USA

SYMPOSIUM PROGRAM

Sponsored by the IEEE Computer Society

Sunday April 7th, 2013

15:00 to 17:00 Registration

17:00 to 19:00 Welcome Reception

Monday April 8th, 2013

8:00 to 8:45 Registration

8:45 to 9:00 Welcome and Introduction

9:00 to 10:00 **SESSION 1: Keynote Talk**

Chair: David W. Matula

High-Precision Computation: Applications and Challenges

David H. Bailey, Lawrence Berkeley Nat.I Lab, USA

10:00 to 10:30 **Coffee break**

10:30 to 12:00 **SESSION 2: Arithmetic Units**

Chair: Stuart Oberman

The Floating-Point Unit of the Jaguar x86 Core

J. Rupley, J. King, E. Quinnell, F. Galloway, K. Patton, P.-M. Seidel, J. Dinh, H. Bui and A. Bhowmik (AMD, USA & India)

Split-path Fused Floating Point Multiply ACcumulate (FPMAC)

S. Srinivasan, K. Budhiya, R. Ramanarayanan, P. S. Babu, T. Jacob, S. Mathew, R. Krishnamurty and V. Errgauntla (Intel India & USA)

FPU Generator for Design Space Exploration

S. Galal, O. Shacham, J. S. Brunhaver, J. Pu, A. Vassiliev and M. Horowitz (Stanford University, USA)

12:00 to 13:30 **Lunch**

13:30 to 15:00 **SESSION 3: Special Session**

Managing Computation, Precision, Accuracy, and Performance on ExaScale Systems

Chair: Eric Schwarz

Precision, Accuracy, Rounding, and Error Propagation

Marius Cornea, Intel Corporation, USA.

Managing the Dense Linear Algebra Software Stack

Robert A. van de Geijn, UT Austin, USA.

Numerical Accuracy and Reproducibility at ExaScale

Hong Diep Nguyen, UC Berkeley, USA.

15:00 to 15:30 **Coffee break**

15:30 to 17:30 **SESSION 4: Domain Specific Designs**

Chair: Paolo Montuschi

Improved Architectures for a Floating-Point Fused Dot Product Unit

J. Sohn and E. Swartzlander (UT Austin, USA)

Floating Point Architecture Extensions for Optimized Matrix Factorization

A. Pedram, R. van de Geijn and A. Gerstlauer (UT Austin, USA)

A Fast Circuit Topology for Finding the Maximum of n k-bit Numbers

B. Yuce, H. F. Ugurdag, S. Goren and G. Dundar (Bogazici University, Ozyegin University & Yeditepe University, Turkey)

A Non-Linear/Linear Instruction Set Extension for Lightweight Ciphers

S. Engels, E. B. Kavun, H. Mihajloska, C. Paar and T. Yalcin (Ruhr-Univ., Germany & Ss Cyril & Methodius Univ., Macedonia)

17:30 to 18:30 **Birds-of-a-Feather: "Arithmetic for Accelerators"**

Tuesday April 9th, 2013

8:45 to 10:00 **SESSION 5: Keynote Talk**

Chair: Neil Burgess

The Antikythera Mechanism and the early history of mechanical computing

Professor M.G. Edmunds, Cardiff University, UK

10:00 to 10:30 **Coffee break**

10:30 to 12:30 **SESSION 6: Verification and Correctness Proofs**

Chair: David Hough

On the componentwise accuracy of complex floating-point division with an FMA

C.-P. Jeannerod, N. Louvet and J.-M. Muller (INRIA Lyon, France)

How to Compute the Area of a Triangle: a Formal Revisit

S. Boldo (Univ. Paris-Sud, France)

SIPE: Small Integer Plus Exponent

V. Lefèvre (INRIA, Lyon, France)

A Formally-Verified C Compiler Supporting Floating-Point Arithmetic

S. Boldo, J.-H. Jourdan, X. Leroy and G. Melquiond (Univ. Paris-Sud & INRIA Paris, France)

12:30 to 14:00 **Lunch**

14:00 to 15:30 **SESSION 7: Modular Arithmetic**

Chair: Peter Kornerup

Fault Detection in RNS Montgomery Modular Multiplication

J. Eynard, F. Gandino and J.-C. Bajard (UPMC Paris, France & Politecnico Torino, Italy)

The unary arithmetical algorithm in bimodular number systems

P. Kurka (Charles Univ. Prague, Czech Rep.) and M. Delacourt (Centro Modelamiento Matematico, Chile)

Parallel modular multiplication on multi-core processors

P. Giorgi, L. Imbert and T. Izard (LIRMM Montpellier, France)

15:30 to 16:00 **Coffee break**

16:00 to 16:30 **Commemoration Luigi Ciminiera and Luigi Dadda**

16:30 to 18:00 **SESSION 8: Floating-Point Error Analysis**

Chair: Sanu Mathew

Comparison between binary64 and decimal64 floating-point numbers

N. Brisebarre, C. Lauter, M. Mezzarobba and J.-M. Muller (ENS Lyon & UPMC Paris, France)

Accurate Parallel Floating-Point Accumulation

E. Kadic, P. Gurniak and A. Dehon (Univ. of Pennsylvania, USA)

Fast Reproducible Floating-Point Summation

H. D. Nguyen and J. Demmel (UC Berkeley, USA)

19:00 **Conference Banquet**

Wednesday April 10th, 2013

8:45 to 10:15 **SESSION 9: Function Approximation**

Chair: Debjit DasSarma

Multiple precision evaluation of the Airy Ai function with reduced cancellation

S. Chevillard (INRIA Sophia Antipolis, France) and M. Mezzarobba (ENS Lyon, France)

Accurate and Fast Evaluation of Elementary Symmetric Functions

H. Jiang (Nat.I Univ. Defense Technology, China), S. Graillat (UPMC Paris, France) and R. Barrio (Univ. Zaragoza, Spain)

Truncated Logarithmic Approximation

M. Sullivan and E. Swartzlander (UT Austin, USA)

10:15 to 10:45 **Coffee break**

10:45 to 12:15 **SESSION 10: Arithmetic in Cryptography**

Chair: Naofumi Takagi

Relation Collection for the Function Field Sieve

J. Detrey, P. Gaudry and M. Videau (Univ. de Lorraine, France)

Another Look at Inversions over Binary Fields

V. Dimitrov (Univ. Calgary, Canada) and K. Järvinen (Aalto University, Finland)

On-the-Fly Multi-Base Recoding for ECC Scalar Multiplication without Pre-Computations

T. Chabrier and A. Tisserand (Univ. Rennes, France)

12:15 to 12:30 **Conference Close and Final Remarks**