

2019 Reed-Muller Workshop

14th International Workshop on Applications of the Reed-Muller Expansion in Circuit Design



***Fredericton, New Brunswick, Canada
May 24, 2019***

This record is provided for the use of workshop attendees only.
All copyright privileges of the papers contained within this record
remain with the authors.

Welcome to the 2019 Reed-Muller Workshop

It is our pleasure to welcome you to the 2019 Reed-Muller Workshop. This is the fourteenth workshop, earlier events having been held in Novi Sad (Serbia) in 2017, Waterloo (Canada) in 2015, Toyama (Japan) in 2013, Tuusula (Finland) in 2011, Naha (Japan) in 2009, Oslo (Norway) in 2007, Tokyo (Japan) in 2005, Trier (Germany) in 2003, Starkville, Mississippi (USA) in 2001, Victoria (Canada) in 1999, Oxford (UK) in 1997, Chiba (Japan) in 1995, and Hamburg (Germany) in 1993. The workshop is an opportunity to share new ideas and challenges in a variety of areas including but not limited to

- Graph-based representations of logic functions: BDD, MDD, BMD, EVBDD, etc.
- EXOR-based representations
- Emerging Technologies: quantum informatics, reversible computing, nano-technology, etc.
- Spectral representation of switching functions
- Graph functions, bent functions, and cryptographic applications
- Implementation in silicon (ASICs, FPLDs, FPGAs, ...)
- Applications of the Reed-Muller transform, including circuit design, processing, etc.
- Cryptographically-significant functions and other applications in cybersecurity

On behalf of all participants, we thank Prof. Vincent Gaudet, University of Waterloo, Canada and Prof. Tsutomu Sasao, Meiji University, Japan for their invited addresses. Their topics of stochastic computing and EXOR logic synthesis, respectively, demonstrate the breadth of topics covered by the workshop.

We thank all the authors of contributed papers and also thank our colleagues on the program committee for their expert reviews and suggestions that have contributed to the quality of the workshop.

Support from the Faculty of Computer Science, University of New Brunswick, Fredericton, NB, Canada and the Darwin Deason Institute for Cybersecurity, Southern Methodist University, Dallas, Texas, USA is gratefully acknowledged as is the assistance of Prof. Gerhard Dueck with local arrangements.

We hope you find the workshop interesting and that it leads to ongoing discussions and collaborations.

Yours sincerely,

Mitchell Thornton, Workshop Chair and *Luca Amaru* and *Michael Miller*, Program Co-chairs

RM2019 Program Committee:

Luca Amaru, Synopsys Inc., USA
Jon Butler, Naval Postgraduate School, USA
Valentina Ciriani, University of Milan, Italy
Rolf Drechsler, University of Bremen, Germany
Elena Dubrova, KTH Royal Institute of Technology, Sweden
Michael Miller, University of Victoria, Canada
Tsutomu Sasao, Meiji University, Japan
Bernd Steinbach, Freiberg University of Mining and Technology, Germany
Mitchell Thornton, Southern Methodist University, USA
Patrick Vuillod, Synopsys Inc., USA
Robert Wille, Johannes Kepler University, Austria

2019 Reed-Muller Workshop

Program

May 24, 2019

Room 122, Gillin Hall

University of New Brunswick

Fredericton, New Brunswick, Canada

09:00 – 09:10 Registration

09:10 – 09:15 Opening Remarks – Mitchell A. Thornton, Workshop Chair

09:15 – 10:15 Invited Address

Stochastic Computing: Tutorial Introduction and Future Prospects, Vincent Gaudet 1

10:15 – 10:45 Nutrition Break

10:45 – 12:15 Session I

Enumerative Analysis of Asymmetric Functions, Jon Butler and Tsutomu Sasao 3

Bent functions, Bent Permutations and a Variety of Methods to Construct Them, 12
Costas Karanikas, Nikolaos Atreas and Radomir Stanković

A Hybrid Spectral Method for Checking Boolean Function Equivalence, 18
Mathias Soeken, Eleonora Testa and Michael Miller

12:15 – 13:30 Lunch

13:30 – 14:30 Invited Address

A Quarter Century of EXOR Logic Synthesis: Memoir, Tsutomu Sasao 26

14:30 – 15:30 Session II

Fixed Polarity Pascal Transforms with Computer Algebra Applications, 34
Mitchell Thornton and Kaitlin Smith

Geometric Refactoring of Quantum and Reversible Circuits: Quantum Layout, 46
Martin Lukac and Georgiy Krylov

15:30 – 16:00 Nutrition Break

16:00 – 16:30 Plenary Session

An open discussion regarding future Reed-Muller Workshops.

Other Contributions

Reed-Muller Representations in Arithmetic Operations, Danila Gorodecky 53