

Record

Reed-Muller Workshop

May 24 – 25, 2017

Novi Sad, Serbia



This record is provided for the convenience of workshop attendees and is not a formal publication. Copyright of the material remains with the authors. Papers from this record should not be distributed further without first seeking permission from the author(s).

Preface

It is our pleasure to welcome you to the 2017 Reed-Muller Workshop being held in Novi Sad, Serbia in conjunction with the 47th annual IEEE International Symposium on Multiple-Valued Logic. This is the 13th workshop which has been held biannually since 1993. Workshop sites have included: Hamburg, Germany (1993); Chiba, Japan (1995); Oxford, UK (1997); Victoria, Canada (1999) Starkville, USA (2001); Trier, Germany (2003); Tokyo, Japan (2005); Oslo, Norway (2007); Naha, Japan (2009); Tuusula, Finland (2011); Toyama, Japan (2013) and Waterloo, Canada (2015).

The quality of a technical meeting such as the Reed-Muller Workshop is primarily dependent on the technical contributions. We thank all researchers who submitted their work and are especially grateful to the Program Committee for their hard work in reviewing the submissions. We thank the authors for their care and attention to the comments of the reviewers while preparing the final versions of the papers appearing in this record. And we thank Smiljana Demay, Dušan Tatić, and Nemanja Jovanović for assistance in preparation of this record.

It is a particular pleasure to express our gratitude to our friend and colleague, Dr. Elena Dubrova, for accepting the invitation to present the opening workshop lecture.

We also wish to thank Prof. Jovanka Pantović and Dr. Dušan Gajić for assistance with the local arrangements for the workshop as well as Shinobu Nagayama and Mathias Soeken for supporting the workshop web site and publicity.

Radomir S. Stanković
RM-2017 Workshop Chair

D. Michael Miller
RM-2017 Program Chair

RM-2017 Program Committee

Jon T. Butler, Naval Postgraduate School, USA
Rolf Drechsler, University of Bremen
Gerhard W. Dueck, University of New Brunswick, Canada
D. Michael Miller (Chair), University of Victoria, Canada
Marek Perkowski, Portland State University, USA
Tsutomu Sasao, Meiji University, Japan
Anatoly Shalyto, ITMO University, Russia
Radomir S. Stanković, University of Niš, Serbia
Bernd Steinbach, Freiberg University of Mining and Technology, Germany
Mitchel A. Thornton, Southern Methodist University, USA
Robert Wille, Johannes Kepler University Austria

Publicity Chair

Mathias Soeken, École Polytechnique Fédérale de Lausanne, Switzerland

Table of Contents

Invited Address

Energy-Efficient Cryptographic Primitives, Elena Dubrova 1

Session 1

Compact XOR-Bi-Decomposition for Generalized Lattices of Boolean Functions 5
Bernd Steinbach and Christian Posthoff

Enumeration and Coding Methods for a Class of Permutations and Reversible Logic Gates 15
Costas Karanikas and Nikolaos Atreas

On the Computation of Reed-Muller Spectra for Cryptography and Switching Theory Applications 21
Mitchell A. Thornton and D. Michael Miller

Session 2

Subsets of Boolean Bent Functions in the Spectral Reed-Muller Domain 33
Miloš Radmanović and Radomir Stanković

Boolean Function Classification with δ -swaps 41
Mathias Soeken, Ina Kodrasi and Giovanni De Micheli

An Improved Walsh Spectral Classification of Boolean Functions for $n \leq 5$ 47
Milena Stanković, Claudio Moraga and Radomir S. Stanković

Session 3

Fundamental Symmetric Boolean Functions and Reed-Muller Spectra 53
Claudio Moraga

BDD and FDD Size Optimization by a Genetic Algorithm 65
Suzana Stojković, Darko Veličković and Claudio Moraga

Cycle Structures of the Reversible Hidden Weighted Bit Function 73
Krzysztof Podlaski

Session 4

Optimal Multiple-Control Toffoli Circuits of Reversible Adder-Subtractors and Reduced Quantum Gate Realization 79
Md. Belayet Ali, Takashi Hirayama, Katsuhisa Yamanaka and Yasuaki Nishitani

An Analytic Sifting Approach to Optimization of LNN Reversible Circuits 87
Martin Lukac, Pawel Kerntopf and Michitaka Kameyama

Plenary Session – Reed-Muller – Past, Present and Future

Early Work in Switching Theory and Logic Design of the Gavrilov School in the Former Soviet Union 93
Anatoly A. Shalyto, Radomir S. Stanković, Jaakko T. Astola and Alexander V. Strukov

A Selected Bibliography on Reed-Muller Representations and Related Topics 103
Radomir S. Stanković and Dragan Janković