FACTA UNIVERSITATIS
Series: **Electronics and Energetics** Vol. 31, N° 2, June 2018, pp. i - iii

GUEST EDITORIAL

The Reed-Muller Workshop has been held biennially since 1993, and since 2007 has been co-located with the IEEE International Symposium on Multiple-valued Logic and supported by the IEEE Computer Society Technical Committee on Multiple-valued Logic. Papers presented at the Workshop are provided informally to attendees but workshop proceedings are not formally published.

The goal of the Reed-Muller Workshop is to provide a forum for researchers to exchange and discuss research ideas in a variety of areas including:

- graph-based representations of logic functions
- EXOR-based representations and spectral representation of logic functions
- graph functions, bent functions, cryptographically-significant functions and cryptographic applications
- implementations in silicon
- applications including circuit design, reversible logic, quantum logic, etc.
- representations for quantum computing, nano-technology, and molecular scale computing

The papers appearing in this issue are from the 2017 Reed-Muller Workshop (RM2017) held May 24-25 in Novi Sad, Republic of Serbia. The first paper in this special issue is the RM2017 invited address ***Energy-Efficient Cryptographic Primitives*** presented by Prof. Elena Dubrova, Royal Institute of Technology (KTH), Stockholm, Sweden. The paper considers how to design cryptographic primitives that address integrity and confidentiality of transmitted messages while satisfying resource constraints. Secondly, this work describes countermeasures which can enhance the resistance of hardware implementing cryptographic algorithms to hardware Trojans.

There are five refereed contributed papers in this special issue. Preliminary versions were presented at RM2017. The papers included here are fully refereed revised and in some cases extended versions.

Genetic Algorithm for Binary and Functional Decision Diagrams Optimization, Suzana Stojković, Darko Veličković and Claudio Moraga, introduces a genetic algorithm to minimize the size, number of nodes, for both Binary Decision Diagrams and Functional Decision Diagrams. Experimental results show the effectiveness of the algorithm particularly when mutation of polarity is introduced for the FDD case.

Compact XOR-Bi-Decomposition for Lattices of Boolean Functions, Bernd Steinbach and Christian Posthoff, presents a method to find a compact XOR-bi-decomposition for a lattice of Boolean functions thereby extending well known techniques for finding AND-, OR-, or XOR-bi-decompositions for a given completely specified function. The approach emphasizes small circuits with low power consumption and delay.

An Improved Spectral Classification of Boolean Functions Based on an Extended Set of Invariant Operations, Milena Stanković, Claudio Moraga and Radomir Stanković, considers the extension of prior spectral methods for the classification of Boolean functions by the introduction of a previously unconsidered invariant operation in the Walsh spectral domain. This work strengthens the classification and resolves a long standing problem in spectral classification. The new invariant operation can also be used in constructing bent functions.

Construction of Subsets of Bent Functions Satisfying Restrictions in the Reed-Muller Domain, Miloš Radmanović and Radomir S. Stanković, considers the important task of determining bent functions which have practical application in cryptography. Three ways of imposing restrictions to construct subsets of Boolean functions which are more readily searched for bent functions are considered. Experimental estimates of the number of bent functions in the corresponding subsets of Boolean functions are given.

Enumeration and Coding Methods for a Class of Permutations and Reversible Logical Gates, Costas Karanikas and Nikolaos Atreas, introduces a variety of coding methods for Boolean sparse invertible matrices and uses these methods to create a variety of bijections on the permutation group $P(m)$ of the set $\{1,2,\ldots,m\}$. It is also shown how several well-known reversible logic gates can be coded by sparse matrices.

The above synopses demonstrate the breadth of research interests covered by the Reed-Muller Workshop ranging from theory to practice including circuit design and cryptography applications.

We express our gratitude to all the authors for their contributions to this special issue. We acknowledge the important contribution of the RM2017 Program Committee and referees, listed below, for their careful review and valuable comments on the contributed papers both for the Workshop and this special issue. We also express our sincere gratitude to Prof. Ninoslav D. Stojadinović, Editor-in-Chief, and Dr. Danijel M. Danković, Technical Secretary, *Facta Universitatis: Electronics and Energetics Series*, for their support of this special issue and for allowing us to serve as guest editors.

This special issue is an excellent venue for dissemination of research results from RM2017. We sincerely hope that publication of these results will stimulate continued research in these important areas.

D. Michael Miller,
University of Victoria, Canada

Tsutomu Sasao,
Meiji University, Japan

RM2017 Program Committee and Referees

Jon. T. Butler	*Naval Postgraduate School, Monterey, USA*
Rolf Drechsler	*University of Bremen, Germany*
Gerhard W. Dueck	*University of New Brunswick, Fredericton, Canada*
Oliver Keszocze	*University of Bremen, Germany*
Alireza Mahzoon	*University of Bremen, Germany*
D. Michael Miller	*University of Victoria, Canada*
Claudio Moraga	*Technical University of Dortmund, Germany*
Philipp Niemann	*University of Bremen, Germany*
Marek Perkowski	*Portland State University, USA*
Tsutomu Sasao	*Meiji University, Kawasaki, Japan*
Anatoly Shalyto	*ITMO University, St. Petersburg, Russia*
Saeideh Shirinzadeh	*University of Bremen, Germany*
Mathias Soeken	*École Polytechnique Fédérale de Lausanne, Switzerland*
Radomir S. Stanković	*University of Niš, Republic of Serbia*
Bernd Steinbach	*TU Universitat Bergakademie Freiberg, Germany*
Mitchel A. Thornton	*Southern Methodist University, Dallas, USA*
Robert Wille	*Johannes Kepler University, Linz, Austria*