Applicable Algebra in Engineering, Communication and Computing (2020) 31:171–172
https://doi.org/10.1007/s00200-020-00436-w

FOREWORD

Special Issue: "Computer Algebra and Application to Combinatorics, Coding Theory and Cryptography" ACA 2019, Montreal, Canada, July 16–20, 2019

Kenza Guenda[1] · Iiro Honkala[2] · Ilias Kotsireas[3] · Teo Mora[4] · Qiang Wang[5]

Published online: 29 May 2020

This volume contains the refereed papers within the scope of the special session on Computer Algebra and Application to Combinatorics, Coding Theory and Cryptography, in the ACA 2019 conference held July 16–20, 2019 at Montreal, Canada. The goal of this special session was to bring together researchers from all areas related to computer algebra (both theoretical and algorithmic), applied combinatorics, coding theory and cryptography, and to provide a stimulating forum where experts can report their recent results and approaches toward various applications, and propose new lines of research to scientific community. There were 14 invited presentations and the organizing committee for the session consisted of Kenza Guenda (Victoria, Canada), Aaron Gulliver (Victoria, Canada), Ilias Kotsireas (Waterloo, Canada), Edgar Martinez Moro (Valladolid, Spain), and Qiang Wang (Ottawa, Canada).

✉ Teo Mora
5919@unige.it

✉ Qiang Wang
wang@math.carleton.ca

Kenza Guenda
ken.guenda@gmail.com

Iiro Honkala
honkala@utu.fi

Ilias Kotsireas
ikotsire@wlu.ca

[1] Department of Electrical and Computer Engineering, University of Victoria,, P.O. Box 1700 STN CSC, Victoria, BC V8W 2Y2, Canada

[2] Department of Mathematics and Statistics, University of Turku, Vesilinnantie 5, 20014 Turku, Finland

[3] CARGO Lab, Wilfrid Laurier University, 75 University Avenue West, Waterloo, ON N2L 3C5, Canada

[4] Dipartimento Di Matematica, Università Di Genova, Via Dodecaneso 35, 16146 Genoa, Italy

[5] School of Mathematics and Statistics, Carleton University, 1125 Colonel By Drive, Ottawa, ON K1S 5B6, Canada

The call for papers welcomed any original paper within the scope and not simultaneously submitted to another journal or conference. Specific topics included, but were not limited to: codes and applications; combinatorial structures; algebraic-geometric codes; network coding; quantum codes; group codes; algebraic cryptanalysis; post-quantum cryptography; code, lattice and hash-based public key cryptography (PKC); multivariate PKC; elimination theory; computational commutative algebra; multivariate polynomial ideal theory; solving systems of algebraic equations; algorithms for computing Gröbner bases.

All eight accepted papers were rigorously refereed according to the journal standards of AAECC and they are listed in alphabetic order by the surname of the first author. These 8 papers covered various topics in computer algebra with applications to combinatorics (e.g., projective planes, SAT problem), coding theory (e.g., error locator polynomials for BCH codes, optimal RS-like LRC codes, skew or repeated-root constacyclic codes), and cryptography (e.g., boomerang uniformity, Gröbner basis, Dickson polynomials, permutation polynomials).

We would like to take this opportunity to thank organizers of ACA 2019 (Michel Beaudin, Anouk Bergeron-Brlek, Louis-Xavier Proulx from École de technologie supérieure) for providing us the venue for our special session. We thank all the speakers (Satya Bagchi, Rama Krishna Bandi, Curtis Bright, Pierre-Louis Cayrel, Michela Ceria, Reza Dastbasteh, Simon Eisenbarth, Kenza Guenda, Daniel J. Katz, Theo Moriarty, Abhay Kumar Singh, Steve Szabo, Merce Villanueva) and all other participants from Canada, France, Germany, India, Ireland, Italy, Spain and USA. We also thank all the referees who spent their valuable time reviewing these papers and providing useful suggestions for their improvement. Finally, we are grateful to the Production Editor Elangovan Ramanathan for his kind help and guidance in the preparation of this special issue.