Cryptography and Communications (2020) 12:819–820
https://doi.org/10.1007/s12095-020-00454-y

Editorial: Special issue on Boolean functions and their applications

Lilya Budaghyan[1] · Tor Helleseth[1]

Published online: 20 August 2020

Mathematics Subject Classification (2010) 68P30

This is the fourth special issue of *Cryptography and Communication* dedicated to Boolean functions and their applications (the previous three appeared in 2016 and 2019 and were associated with the events of BFA 2014, BFA 2017 and BFA 2018).

In June 2019, specialists from 15 different countries all over the world gathered in Florence, Italy, at the International Workshop on Boolean Functions and Their Applications BFA 2019, the event celebrating the 70th birthday of Claude Carlet.

Prof. Carlet (University of Paris 8 and University of Bergen) is a well-known scientist who has made a considerable contribution to the fields of Boolean functions, cryptography, coding theory, finite fields and sequence design. In particular, he is one of the founders of cryptographic Boolean functions theory.

BFA 2019 had 15 invited speakers including Marco Calderini, Claude Carlet, Robert Coulter, Ulrich Dempwolff, Daniel Katz, Chunlei Li, Nian Li, Sihem Mesnager, Daniel Panario, Emmanuel Prouff, Chunming Tang, Alev Topuzoglu and Yuyin Yu. Contributed talks were also presented at the workshop. The presented talks highlighted recent results in the field which covered various applications of Boolean functions including coding, cryptography, sequence design, combinatorics, commutative algebra and discrete mathematics. All speakers have been invited to submit a paper (on the subject of their talk or another subject connected to Boolean functions). All received submissions were thoroughly reviewed and 13 papers, described below, have been accepted after revision.

This special issue is dedicated to the 70th Birthday of Claude Carlet

This article belongs to the Topical Collection: *Boolean Functions and Their Applications IV*

✉ Lilya Budaghyan
Lilya.Budaghyan@uib.no

Tor Helleseth
Tor.Helleseth@uib.no

[1] Department of Informatics, University of Bergen, PO Box 7803, 5020 Bergen, Norway

Boolean functions are used in cryptography, in particular in block and stream ciphers. An important condition on these functions is a high resistance to the differential and linear cryptanalyses, which are measured by differential uniformity and nonlinearity of functions, respectively. Bent, almost bent, perfect nonlinear and almost perfect nonlinear (APN) functions are those which show optimality in respect to one or both of the above mentioned properties.

'On the EA-classes of known APN functions in small dimensions' (Calderini), 'The multivariate method strikes again: New power functions with low differential uniformity in odd characteristic' (Felke) and 'On the linear structures of balanced functions and quadratic APN functions' (Musukwa and Sala) are dedicated to functions with optimal or near optimal differential uniformity.

Results on functions with optimal nonlinearity are presented in the papers 'The group of automorphisms of the set of self-dual bent functions' (Kutsenko) and 'Vectorial bent functions in odd characteristic and their components' (Meidl, Çeşmelioğlu and Pott).

Further cryptographic properties of Boolean functions are studied in the papers 'Permutation polynomials and factorization' by Kalaycı, Stichtenoth & Topuzoğlu), 'Boolean functions with multiplicative complexity 3 and 4' (Çalık, Turan and Peralta) and 'Cryptographic properties of small bijective S-boxes with respect to modular addition' (Zajac and Jókay).

Application of Boolean functions to coding theory is in the papers 'Recent results and problems on constructions of linear codes from cryptographic functions' (Li and Mesnager) and 'On decoding additive generalized twisted Gabidulin codes' (Kadir and Li).

Mathematical techniques for analysing Boolean functions are presented in 'Combinatorial t-designs from special functions' (Ding and Tang), 'Root-Hadamard transforms and complementary sequences' (Stanica), and 'A note on the distinctness of some Kloosterman sums' (Borissov).

We thank all the authors of these papers for their nice contributions, and also the large number of reviewers whose careful reading of the papers have ensured the high standard of this special issue.