Cryptography and Communications (2019) 11:1–2
https://doi.org/10.1007/s12095-018-0341-2

Editorial: Special Issue on Boolean functions and their applications

Lilya Budaghyan[1] · Claude Carlet[1] · Tor Helleseth[1]

Published online: 14 November 2018

Many problems in the domains of cryptography, coding theory, sequence theory and circuit theory can be formulated in terms of Boolean functions. The connections between these domains and Boolean functions, and between these domains through Boolean functions, are numerous. The present special issue of the Journal "Cryptography and Communications" is devoted to them.

A first example of such connection is with substitution boxes (S-boxes) and their nonlinearity and differential uniformity (including the notion of APNness). These notions come from cryptography, but also play an important role in sequence theory and are closely related to important issues in coding theory. The papers "On APN functions $L_1(x^3) + L_2(x^9)$ with linear L_1 and L_2" by Irene Villa, "On an algorithm generating 2-to-1 APN functions and its applications to the Big APN problem", by Valeriya Idrisova and "Cellular Automata Based S-boxes" by Luca Mariot, Stjepan Picek, Alberto Leporati and Domagoj Jakobovic deal with the generation of vectorial functions having such good features.

A second example is with the notions of nonlinearity of Boolean functions and of bent functions, whose definitions come from cryptography as well, but are also connected to coding theory through Kerdock codes and to (bent) sequences. The papers "On the nonlinearity of Boolean functions with restricted input" by Sihem Mesnager, Zhengchun Zhou and Cunsheng Ding and "New classes of p-ary bent functions" by Bimal Mandal, Pantelimon Stănică and Sugata Gangopadhyay study further these notions, with additional constraints and extended to other characteristics.

The circuit complexity plays an important role in all applicative domains of Boolean functions. The papers "The Multiplicative Complexity of 6-variable Boolean Functions" by

This article is part of the Topical Collection on *Special Issue on Boolean Functions and Their Applications*

✉ Lilya Budaghyan
Lilya.Budaghyan@uib.no

Claude Carlet
claude.carlet@gmail.com

Tor Helleseth
Tor.Helleseth@uib.no

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

Çağdaş Çalik, Meltem Sönmez Turan and René Peralta, and “Small Low-Depth Circuits for Cryptographic Applications” by Joan Boyar, Magnus Gausdal Find and René Peralta study these circuit issues with a cryptographic viewpoint.

Permutation polynomials are important for generating S-boxes, bent functions through the Maiorana-McFarland construction and APN functions. The paper “New permutation trinomials from Niho exponents over finite fields with even characteristic” by Nian Li and Tor Helleseth revisit in the framework of such bijections over finite fields a structure introduced by Niho in sequence theory which has also played an important role in another construction of bent functions.

In June 2017, we invited leading specialists from ten different countries all over the world in Sosltrand Hotel, Os, Norway.[1] Contributed papers were also presented. All speakers have been invited to submit a paper (on the subject of their talk or on another subject connected to Boolean functions). All received submissions were thoroughly reviewed and eight papers have been accepted after revision among the eleven submitted.

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.

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

[1] Information on BFA 2017 can be found on the webpage https://people.uib.no/chunlei.li/workshops/BFA2017/