Editorial: Special issue on Boolean functions and their applications 2020

Lilya Budaghyan¹ · Claude Carlet^{1,2} · Tor Hellese¹ · Kaisa Nyberg³

Accepted: 27 August 2021 / Published online: 26 October 2021

© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2021

Mathematics Subject Classification (2010) 00B15

This is the fifth special issue of *Cryptography and Communications* dedicated to Boolean functions and their applications. The previous four appeared in 2016, 2019, 2020 (with two issues in 2019) and were associated with the events of BFA 2014, BFA 2017, BFA 2018, BFA 2019.

In September 2020, the International Workshop on Boolean Functions and Their Applications BFA 2020 took place in Loen, Norway. This event also served for announcement of the first winner of the George Boole International Prize established to recognize outstanding contributions in the domain of Boolean functions and related fields. The invited speakers of the workshop included the recipient of the prize, Sihem Mesnager from the University of Paris VIII, and seven other leading researchers in the field of Boolean functions: Cunsheng Ding from Hong Kong University of Science and Technology, Faruk Göloğlu from Charles University in Prague, Nikolay Kaleyski from the University of Bergen, Daniel Katz

This article belongs to the Topical Collection: *Boolean Functions and Their Applications V*
Guest Editors: Lilya Budaghyan, Claude Carlet, Tor Hellese and Kaisa Nyberg

✉ Lilya Budaghyan
Lilya.Budaghyan@uib.no

Claude Carlet
claud.carlet@gmail.com

Tor Hellese
Tor.Hellese@uib.no

Kaisa Nyberg
kaisa.nyberg@aalto.fi

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

² Department of Mathematics, University of Paris 8, 2 rue de la liberté, 93526 Saint-Denis, Cedex, France

³ Department of Computer Science, Aalto University, P.O. Box 15400, FI-00076, Aalto, Finland

from California State University Northridge, Svetla Nikova from the KU Leuven, Léo Perrin from INRIA France, Kai-Uwe Schmidt from Paderborn University. Contributed talks were also presented at the workshop. 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 8 papers, described below, have been accepted after revision.

The paper “Kim-type APN functions are affine equivalent to Gold functions” by Benjamin Chase and Petr Lisonek is dedicated to the so-called Big APN problem on the existence of APN permutations of $\mathbb{F}_{2^{2n}}$ for even $n > 6$. Motivated by the Kim function that had led to the APN permutation over $\mathbb{F}_{2^6}$, Claude Carlet raised a problem on finding new Kim-type APN functions. The authors provide a negative solution to this problem by proving that such functions are always affine equivalent to Gold functions.

EA- and CCZ-equivalence are two main forms of equivalence for vectorial Boolean functions used in cryptography. The paper “Invariants for EA- and CCZ-equivalence of APN and AB functions” by Nikolay Kaleyski is a survey of all the invariants that are currently known for these forms of equivalence.

While the classical differential uniformity is invariant under CCZ-equivalence, the newly defined concept of c -differential uniformity, in general is not invariant under EA- or CCZ-equivalence. In the paper “Characters, Weil sums and c -differential uniformity with an application to the perturbed Gold function”, Pantelimon Stanica, Constanza Riera and Anton Tkachenko study how the c -differential uniformity of the classical “good” functions behave when adding some linearized terms.

The paper “Resilient Uniformity: Applying Resiliency in Masking” by Siemen Dhooghe and Svetla Nikova deals with the important cryptographic issue of side channel attacks and specifically with the counter-measure called threshold implementation (TI), which is efficient for ensuring first order security but whose extension to higher order security is problematic. The paper introduces a new notion, called resilient uniformity, and shows how TI can provide second order protection.

When a Boolean function is used in a construction of a symmetric cipher it is required to be balanced. In some cases also a stronger property may be required, that is, the Boolean function must be balanced when restricted to subsets of fixed Hamming weight. Such functions are said to be weightwise perfectly balanced (WPB). Very few examples of WPB functions are known so far. The article by Sihem Mesnager and Sihong Su “On constructions of weightwise perfectly balanced Boolean functions” presents and studies two new constructions of WPB functions.

The paper “On properties of a bent function secondary construction”, by Nikolay Kolomeec revisits the idea which led to the thirty year old classes of bent Boolean functions called C and D ; it studies further when the addition of the indicator of an affine subspace of arbitrary dimension to a given bent function preserves its bentness and compares what happens for a bent function and its dual.

Linear codes have many important applications in cryptography and security. In particular they can be used to construct practical secret sharing schemes. The paper “Secret sharing schemes based on the dual of Golay codes” by Jian Ding, Changlu Lin and Sihem Mesnager proposes two secret sharing schemes based on the dual of the $[23, 12, 7]_2$ and $[11, 6, 5]_3$ Golay codes. The minimal access structures of these schemes are determined and they are shown to be 3-democratic.

The study of t -designs has a long history in combinatorics. The incidence matrix of a t -design generates a linear code. The paper "The linear codes of t -designs held in the Reed-Muller codes and Simplex codes" by Cunsheng Ding and Chunming Tang considers the linear codes of t -designs held in these codes. In addition to some general theory for linear codes of t -designs held in linear codes, the paper presents several open problems.

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.