Editorial: Special issue on Boolean functions and their applications 2018

Lilya Budaghyan¹ · Claude Carlet¹ · Tor Helleseeth¹

Published online: 4 November 2019

© Springer Science+Business Media, LLC, part of Springer Nature 2019

This is the third special issue of *Cryptography and Communications* dedicated to Boolean functions and their applications (the previous two appeared in 2016 and 2019 and were associated with the events of BFA 2014 and BFA 2017). Boolean functions (single-output and multi-output ones) are used in the design of stream and block ciphers and in the definition of some important error correcting codes; they are also directly related to some problems on sequences for telecommunications. In June 2018, we invited leading specialists from nine different countries all over the world to Loen, Norway, for the international workshop on Boolean functions and their applications BFA 2018. All speakers have been invited to submit a paper. All the papers sent were thoroughly reviewed and twelve papers, described below, have been accepted after revision.

In cryptography, S(substitution)-boxes are core components in symmetric ciphers. In order for the algorithm to resist one of the most prominent cryptanalytic techniques, namely differential attacks [13], S-boxes should have a low differential uniformity. APN functions are optimal in this respect. The paper “If a Generalised Butterfly is APN then it Operates on 6 Bits” by Anne Canteaut, Léo Perrin and Shizhu Tian is dedicated to a very important problem on the existence of APN permutations over $\mathbb{F}_{2^{2n}}$ and it proves that a recently introduced generalised butterfly construction using Gold exponents can never be APN for $n > 3$.

Continuing the work of Budaghyan, Carlet, Helleseeth, Li and Sun on finding conditions when a resulting function after changing one value in an APN function is APN itself, Nikolay Kaleyski studies a similar problem for the case of changing two values in the paper “Changing APN Functions at Two Points”.

Algebraic attacks are a powerful technique for the cryptanalysis of stream ciphers. The algebraic immunity of Boolean functions quantifies their contribution to the resistance

✉ Lilya Budaghyan
Lilya.Budaghyan@uib.no

Claude Carlet
Claude.Carlet@gmail.com

Tor Helleseeth
Tor.Helleseeth@uib.no

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

against these attacks. In some applications, Boolean functions are used over subsets of $\mathbb{F}_2^n$ instead of $\mathbb{F}_2^n$ itself. In “A Family of Weightwise (Almost) Perfectly Balanced Boolean Functions with Optimal Algebraic Immunity”, Deng Tang and Jian Liu propose a large family of Boolean functions which maintain their good cryptographic properties, like balancedness and large algebraic immunity, when the input is restricted to some subsets.

The following two papers are dedicated to permutation polynomials, an important topic in finite fields. The paper “On a Class of Permutation Trinomials in Characteristic 2” by Xiang-Dong Hou provides another proof to the Tu-Zeng-Li-Helleseth conjecture on permutation polynomials of special trinomial form. Claude Gravel, Daniel Panario and David Thomson introduce a new construction of permutations with special cyclic properties, high algebraic degrees and large number of terms in their ANF in their article “Unicyclic strong permutations”.

The bentness of Boolean functions is an important notion, which has been generalized to functions over fields and rings larger than $\mathbb{F}_2$. As described by the titles, constructions and properties of generalized bent functions are investigated in the papers “Generalized bent functions into Z_{p^k} from the partial spread and the Maiorana-McFarland class” by Wilfried Meidl and Alexander Pott, and “Multiple Characters Transforms and Generalized Boolean Functions” by Sihem Mesnager, Constanza Riera and Pantelimon Stănică. In “Several new classes of self-dual bent functions derived from involutions”, Gaojun Luo, Xiwang Cao and Sihem Mesnager study the subclass of those bent functions, called self dual bent functions, which are equal to their dual. They provide two methods for constructing such functions and several new classes are produced. In “Frobenius linear translators giving rise to new infinite classes of permutations and bent functions”, N. Cepak, E. Pasalic and A. Muratovic-Ribic derive new bent functions from new permutations.

Functions over finite fields have diverse applications to the construction of other interesting mathematical objects. In the paper “Strongly Regular Graphs Arising from Non-Weakly Regular Bent Functions”, Ferruh Özbudak and Rumi Melih Pelen study subsets of a finite field of odd characteristic associated with non-weakly regular bent functions in relation to partial difference sets. The paper “Image Sets with Regularity of Differences” by Patrick G. Cesarz and Robert S. Coulter presents a new approach to constructing sets with regularity of differences, and, in particular, the use of functions over finite fields exhibiting a regularity of images.

Multiplicative complexity (MC) is an important parameter of Boolean functions and the implementation cost of various secure cryptographic implementations is often proportional to the MC of underlying Boolean functions. Luís Brandão, Çağdaş Çalik, Meltem Sönmez Turan and René Peralta study the MC of symmetric Boolean functions in the paper “Upper Bounds on the Multiplicative Complexity of Symmetric Boolean Functions”.

Acknowledgments 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.