Editorial: Special issue on Boolean functions and their applications

Lilya Budaghyan¹ · Tor Hellese¹ ·
Alexander Kholosha¹

Published online: 28 November 2015
© Springer Science+Business Media New York 2015

The notion of a Boolean function was introduced in the second half of the nineteenth century in the context of fundamental mathematics and mathematical logic. It was named after George Boole (1815–1864), an English mathematician, who was one of the founders of mathematical logic. Since the middle of the twentieth century, with the rapid development of information and communication technology, Boolean function theory has been an important tool for solving problems of analysis and synthesis of discrete devices which transform and process information. In particular, many cryptographic problems are formulated in terms of Boolean functions and Boolean function techniques are essential for solving these problems.

In September 2014 we invited leading specialists from eleven different countries all over the world to the International Workshop on Boolean Functions and Their Applications BFA 2014 which took place in Rosendal, Norway¹. The participants presented talks highlighting recent results in the field which covered various applications of Boolean functions including coding, cryptography, combinatorics, commutative algebra and algebraic geometry. After the workshop all participants of BFA 2014 were invited to submit a paper to this special issue of the Journal “Cryptography and Communications”. All received submissions were thoroughly reviewed using the high reviewing standard of this journal and the following seven papers in this volume are the end results of the selection process.

---

¹Information on BFA 2014 can be found on the workshop webpage
<http://www.people.uib.no/lbu061/BFA2014.html>

✉ L. Budaghyan
Lilya.Budaghyan@uib.no

T. Hellese¹
Tor.Hellese@uib.no

A. Kholosha
Alexander.Kholosha@uib.no

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

The paper by Phillipe Langevin and Daniel Katz “New open problems related to old conjectures by Helleseeth” surveys some recent results on the Fourier spectra of power permutations over finite fields, and poses new open problems related to Helleseeth’s conjectures from the mid-seventies.

In the paper “Spectra of a class of quadratic functions: average behavior and counting functions” Wilfried Meidl, Canan Kasikci and Alev Topuzoglu study Walsh spectra of quadratic functions from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ with all coefficients in $\mathbb{F}_p$ where p is a prime. They also survey some known methods and results for constructing and enumerating these functions with given Walsh spectra.

Chunlei Li and Tor Helleseeth study covering radii of linear codes corresponding to planar and APN functions, and, consequently, construct classes of p -ary quasi-perfect codes for p an odd prime, in their paper “Quasi-perfect linear codes from planar and APN functions”.

The paper “Further constructions of infinite families of bent functions from new permutations and their duals” by Sihem Mesnager exhibits new infinite families of bent functions with their dual functions. Some of these bent functions are obtained via new infinite families of permutations provided with their compositional inverses.

In the paper on “Reversed genetic algorithms for generation of bijective S-boxes with good cryptographic properties”, Georgi Ivanov, Nikolay Nikolov, and Svetla Nikova consider the important problem of constructing nonlinear components for block ciphers which are essential in ensuring resistance to cryptanalysis. The linear redundancy is among the considered properties.

In their paper “Influence of addition modulo 2” on algebraic attacks” Oleksandr Kazymyrov, Roman Oliynykov and Håvard Raddum present improved algebraic cryptanalysis of 8-round and 14-round reduced versions of the GOST block cipher. Their method is based on establishing efficiently representable linear systems of equations between known plaintext bits and ciphertext bits and unknown key bits. Such systems can be constructed using Binary Decision Diagrams (BDDs).

In the paper “Enhanced criteria on differential uniformity and nonlinearity of cryptographically significant functions” Yin Tan, Guang Gong and Bo Zhu generalized the notions of differential uniformity and nonlinearity and showed that some known ciphers have poor performance under the generalized criteria.

Finally, we would like to thank the authors for their contributions and the large number of reviewers whose careful reading of these papers have ensured that this special issue is of a high standard.