Cryptography and Communications (2023) 15:1049–1051
https://doi.org/10.1007/s12095-023-00678-8

Editorial: Special issue on Boolean functions and their applications 2022

Lilya Budaghyan[1] · Claude Carlet[1,2] · Tor Helleseth[1] · Wilfried Meidl[3]

Published online: 21 October 2023

Mathematics Subject Classification (2010) 00B15 · 11T71 · 11T06

This is the seventh special issue of Cryptography and Communications dedicated to Boolean functions and their applications. It consists of 10 papers, described below.

In the paper by Li-An Chen and Robert Coulter, an upper bound on the differential uniformity for a class of polynomials over finite fields of odd characteristic is established. In particular a class of permutation polynomials over fields of size 3 modulo 4 with differential uniformity at most 5 is given. There are many results in the literature on permutation polynomials with low differential uniformity over finite fields of characteristic 2, and on polynomials over finite fields of odd characteristic with differential uniformity 1 (planar functions), which cannot be a permutation. So far there are not many results on permutation polynomials in odd characteristic with low differential uniformity.

The paper by Robert Christian Subroto, is motivated by the observation that the linear layer used in the cipher Subterranean 2.0 has relatively low order. The author presents a mathematical framework based on abstract algebra to study the algebraic structure of linear layers of a form similar to the layer used in Subterranean 2.0. Based on this analysis two examples with significantly higher order are constructed.

Due to the general difficulty of constructing and analysing APN functions, weaker notions of APN-ness, like 0-APN-ness, have been introduced. In the paper by Nikolay Kaleyski, Kjetil Nesheim, Pantelimon Stănică, For an infinite family of exponents $d = e(l, k)$ (depending on the parameters l, k), sufficient conditions for which x^d is 0-APN are derived. All cases are

✉ Lilya Budaghyan
Lilya.Budaghyan@uib.no

Claude Carlet
Claude.Carlet@univ-paris8.fr; Claude.Carlet@gmail.com

Tor Helleseth
Tor.Helleseth@uib.no

Wilfried Meidl
meidlwilfried@gmail.com

[1] University of Bergen, Bergen, Norway

[2] University of Paris 8, Paris, France

[3] Johann Radon Institute for Computational and Applied Mathematics, Linz, Austria

characterized in which $e(l, k)$ can be cyclotomic equivalent to one of the six known APN exponents (Gold, Welch, Kasami, Niho, Dobbertin and the inverse exponent). Computationally it is shown that for small values of l and k and finite fields $\mathbb{F}_{2^n}$, $n \leq 100$, there are no APN monomials x^d, $d = e(l, k)$, outside the known classes. This supports the conjecture that the six known APN exponents are the only ones up to equivalence.

The algebraic degree is an important parameter for Boolean functions. If a Boolean function is not given with its algebraic normal form, it is in general not easy to estimate the algebraic degree. In the article by Ana Sălăgean, Percy Reyes-Paredes, a probabilistic test is proposed for deciding whether the algebraic degree of a Boolean function is below a certain value k, which a function of algebraic degree at most k always passes. Results on the probability for a function of degree larger than k to fail the test are presented. It is shown that in particular if the algebraic degree is exactly k, then this probability is not small so that a small number of rounds is sufficient to give the correct result with a high probability.

In the article by Ana Sălăgean, Ferruh Özbudak, research on a recent generalization of almost perfect nonlinear functions for odd characteristic is pushed forward. All those monomial functions on $\mathbb{F}_{p^n}$ for which the exponent has exactly two non-zero digits when represented in base p, and which are generalized almost perfect nonlinear functions (GAPN), are completely characterized. A family of GAPN functions on $\mathbb{F}_{p^3}$ of algebraic degree p is given explicitly.

A number of cryptographic primitives, e.g. KEECAK, XOODOO; SUBTERRANEAN make use of a non-linear mapping, which is called χ mapping. In the article by Silvia Mella, Alireza Mehrdad, Joan Daemen, differential and linear propagation properties of the χ function are analysed. These properties are crucial for functions used in ciphers to thwart differential and linear attacks. In particular, a method to compute the number of linear approximations of χ with given correlation is presented. Based on this method, results on the distribution of linear approximations of some permutations whose non-linear layer is based on χ are obtained.

In the paper by Valerie Gillot, Phiippe Langevin, the authors present a procedure to determine the number $n(s, t, m)$ of pairwise affine inequivalent Boolean functions modulo the Reed-Muller code $RM(s - 1, m)$ in $m = 7$ variables and algebraic degree at most t, $s \leq t \leq 7$. This provides a classification of the set $B(s, t, 7)$ of Boolean functions in 7 variables of algebraic degree t and lowest degree term at least s. In particular with the classification of $B(3, 4, 7)$, respectively of $B(4, 7, 7)$, the classification of semibent functions, respectively an alternative method to determine the covering radius of $RM(3, 7)$ is obtained.

The article by Jyotitmoy Basak, Subhamoy Maitra, Prabal Paul, Animesh Roy, provides an exhaustive study of all Boolean functions in four variables to express binary input binary output two-party nonlocal games and explores their performance in both classical and quantum scenarii. In particular it is noted that the "CHSH game" is the most efficient in terms of separation between quantum and classical techniques.

The article by Marko Djurasevic, Domagoj Jakobovic, Luca Mariot, Stjepan Picek, surveys the metaheuristic approaches used to construct Boolean functions with good cryptographic properties in the literature by providing a new taxonomy. In particular, those approaches are divided into direct design and metaheuristic-assisted design of Boolean functions, where the former is further divided into truth table-based and Walsh-Hadamard-based approaches, and the latter is interpreted in terms of the evolution of algebraic constructions and the optimization of combinatorial objects related to Boolean functions.

The paper by Nurdagül Anbar, Tekgül Kalaycı, and Wilfried Meidl considers the notion of generalized semifield spread to construct bent functions and to study their behavior with respect to isotopisms.

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.