Abdukhalikov, Kanat; Mesnager, Sihem
Bent functions linear on elements of some classical spreads and presemifields spreads.
(English) Zbl 1354.51015

Summary: Bent functions are maximally nonlinear Boolean functions with an even number of variables.
They have attracted a lot of research for four decades because of their own sake as interesting combinatorial objects,
and also because of their relations to coding theory, sequences and their applications in cryptography and other domains such as design theory.
In this paper we investigate explicit constructions of bent functions which are linear on elements of spreads. After presenting an overview on this topic,
we study bent functions which are linear on elements of presemifield spreads and give explicit descriptions of such functions for known commutative presemifields. A direct connection between bent functions which
are linear on elements of the Desarguesian spread and oval polynomials over finite fields was proved by C. Carlet
and the second author [J. Comb. Theory, Ser. A 118, No. 8, 2392–2410 (2011; Zbl 1236.94052)].
Very recently, further nice extensions have been made by C. Carlet [More PS and $H$-like bent functions.
Cryptography ePrint Archive Report 2015/168 (2015)] in another context. We introduce oval polynomials for semifields which are dual to symplectic semifields. In particular, it is shown that from a linear oval polynomial for a semifield one can get an oval polynomial for transposed semifield.

MSC:
51E23 Spreads and packing problems in finite geometry
12K10 Semifields
94A60 Cryptography

Keywords:
Boolean functions; bent functions; Walsh Hadamard transform; spreads; quasifields; semifields; symplectic semifields; oval polynomials

Full Text: DOI

References:
  · Zbl 1317.05024 · doi:10.1007/s10801-014-0565-y
  · Zbl 1101.94021 · doi:10.1016/j.dam.2005.03.027
  · Zbl 1209.94035
[5] Carlet, C; Mesnager, S, On dillon’s class H of bent functions, niho bent functions and o-polynomials, J. Comb. Theory, Ser. A,
  · doi:10.1007/s10623-015-0145-8
  · Zbl 1361.11079 · doi:10.1137/140963273
  · doi:10.1016/j.disc.2016.03.029
This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original paper as accurately as possible without claiming the completeness or perfect precision of the matching.