Martinsen, Thor; **Meidl, Wilfried**; **Stănică, Pantelimon**
Partial spread and vectorial generalized bent functions. (English) Zbl 1408.94997
Des. Codes Cryptography 85, No. 1, 1-13 (2017).

Summary: In this paper we generalize the partial spread class and completely describe it for generalized Boolean functions from $\mathbb{F}_2^n$ to $\mathbb{Z}_{2^t}$. Explicitly, we describe gbent functions from $\mathbb{F}_2^n$ to $\mathbb{Z}_{2^t}$, which can be seen as a gbent version of Dillon's PS_{ap} class. For the first time, we also introduce the concept of a vectorial gbent function from $\mathbb{F}_2^n$ to $\mathbb{Z}_q^m$, and determine the maximal value which m can attain for the case $q = 2^t$. Finally we point to a relation between vectorial gbent functions and relative difference sets.

MSC:

94C10 Switching theory, application of Boolean algebra; Boolean functions (MSC2010)
06E30 Boolean functions
05B10 Combinatorial aspects of difference sets (number-theoretic, group-theoretic, etc.)

Keywords:

generalized Boolean function; generalized bent function; partial spread; vectorial function; relative difference set

Full Text: DOI arXiv

References:

[1] Çeşmelioğlu, A; McGuire, G; Meidl, W, A construction of weakly and non-weakly regular bent functions, J. Combin. Theory Ser. A, 119, 420-429, (2012) · Zbl 1258.94034 · doi:10.1016/j.jcta.2011.10.002

[2] Çeşmelioğlu A., Meidl W., Pott A.: Vectorial bent functions and their duals (manuscript). · Zbl 1361.11079

[3] Dillon J.F.: Elementary Hadamard difference sets. Ph.D. dissertation, University of Maryland (1974). · Zbl 0346.05003

[4] Hodžić, S; Pasalic, E, Generalized bent functions—some general construction methods and related necessary and sufficient conditions, Cryptogr. Commun., 7, 469-483, (2015) · Zbl 1343.94064 · doi:10.1007/s12095-015-0126-9

[5] Kantor W.: Bent functions generalizing Dillon's partial spread functions. arXiv:1211.2600v1. · Zbl 1367.94410

[6] Kumar, PV; Scholtz, RA; Welch, LR, Generalized bent functions and their properties, J. Combin. Theory Ser. A, 40, 90-107, (1985) · Zbl 0585.94016 · doi:10.1016/0097-3165(85)90049-4

[7] Lisonek, P; Lu, YH, Bent functions on partial spreads, Des. Codes Cryptogr., 73, 209-216, (2014) · Zbl 1355.94104 · doi:10.1007/s10623-013-9820-9

[8] Martinsen T., Meidl W., Stănică P.: Generalized bent functions and their Gray images. In: Proceedings of WAIFI (Gent 2016). Lecture Notes in Computer Science (to appear). · Zbl 1409.11135

[9] Nyberg K.: Perfect nonlinear S-boxes. In: Davies D.W. (ed.) Advances in Cryptology, EUROCRYPT '91 (Brighton, 1991). Lecture Notes in Computer Science, vol. 547, pp. 378-386. Springer, Berlin (1991) · Zbl 0766.94012

[10] Rothaus, OS, On "bent" functions, J. Combin. Theory Ser. A, 20, 300-305, (1976) · Zbl 0336.12012 · doi:10.1016/0097-3165(76)90024-8

[11] Schmidt, KU, Quaternary constant-amplitude codes for multicode CDMA, IEEE Trans. Inform. Theory, 55, 1824-1832, (2009) · Zbl 1367.94344 · doi:10.1109/TIT.2009.2013041

[12] Schmidt, KU, ${\mathbb{Z}}_4$-valued quadratic forms and quaternary sequence families, IEEE Trans. Inform. Theory, 55, 5803-5810, (2009) · Zbl 1367.94410 · doi:10.1109/TIT.2009.2032818

[13] Stănică, P; Martinsen, T; Gangopadhyay, S; Singh, BK, Bent and generalized bent Boolean functions, Des. Codes Cryptogr., 69, 77-94, (2013) · Zbl 1322.94094 · doi:10.1007/s10623-012-9622-5

[14] Tan, Y; Pott, A; Feng, T, Strongly regular graphs associated with ternary bent functions, J. Combin. Theory Ser. A, 117, 668-682, (2010) · Zbl 1267.05300 · doi:10.1016/j.jcta.2009.05.003

[15] Tang C., Xiang C., Qi Y., Feng K.: Complete characterization of generalized bent and 2^k-bent Boolean functions. https://eprint.iacr.org/2016/335. · Zbl 1370.94614

[16] Zhang, WG; Pasalic, E, Highly nonlinear balanced S-boxes with good differential properties, IEEE Trans. Inform. Theory, 60, 7970-7979, (2014) · Zbl 1359.94634 · doi:10.1109/TIT.2014.2360880