Kutsenko, Aleksandr

Metrical properties of self-dual bent functions. (English) Zbl 07149379

Des. Codes Cryptography 88, No. 1, 201-222 (2020).

Summary: In this paper we study metrical properties of Boolean bent functions which coincide with their dual bent functions. We propose an iterative construction of self-dual bent functions in $n+2$ variables through concatenation of two self-dual and two anti-self-dual bent functions in n variables. We prove that minimal Hamming distance between self-dual bent functions in n variables is equal to $2^{n/2}$. It is proved that within the set of sign functions of self-dual bent functions in $n \geq 4$ variables there exists a basis of the eigenspace of the Sylvester Hadamard matrix attached to the eigenvalue $2^{n/2}$. Based on this result we prove that the sets of self-dual and anti-self-dual bent functions in $n \geq 4$ variables are mutually maximally distant. It is proved that the sets of self-dual and anti-self-dual bent functions in n variables are metrically regular sets.

MSC:

06E30 Boolean functions
15B34 Boolean and Hadamard matrices
94C10 Switching theory, application of Boolean algebra; Boolean functions (MSC2010)

Keywords:

Boolean functions; self-dual bent; iterative construction; metrical regularity

Full Text: DOI

References:

[1] Canteaut, A.; Charpin, P., Decomposing bent functions, IEEE Trans. Inf. Theory, 49, 8, 2004-2019 (2003) · Zbl 1184.94230

[2] Carlet, C.; Crama, Y.; Hammer, Pl, Boolean functions for cryptography and error correcting code, Boolean Models and Methods in Mathematics, Computer Science, and Engineering, 257-397 (2010), Cambridge: Cambridge University Press, Cambridge

[3] Carlet, C.; Danielson, Le; Parker, Mg; Solé, P., Self-dual bent functions, Int. J. Inform. Coding Theory, 1, 384-399 (2010) · Zbl 1204.94118

[4] Carlet, C.; Mesnager, S., Four decades of research on bent functions, J. Des. Codes Cryptogr., 78, 1, 5-50 (2016) · Zbl 1378.94028

[5] Climent, Joan-Josep; García, Francisco J.; Requena, Verónica, A Construction of Bent Functions ofn+2Variables from a Bent Function ofnVariables and Its Cyclic Shifts, Algebra, 2014, 1-11 (2014) · Zbl 1327.94038

[6] Cusick, Tw; Stănică, P., Cryptographic Boolean Functions and Applications (2017), London: Academic Press, London

[7] Danielsen, Lars Eirik; Parker, Matthew G.; Solé, Patrick, The Rayleigh Quotient of Bent Functions, Cryptography and Coding, 418-432 (2009), Berlin, Heidelberg: Springer Berlin Heidelberg, Berlin, Heidelberg · Zbl 1234.06010

[8] Dillon J.: Elementary Hadamard difference sets. PhD. dissertation, Univ. Maryland, College Park (1974). · Zbl 0346.05003

[9] Feulner, T.; Sok, L.; Solé, P.; Wassermann, A., Towards the classification of self-dual bent functions in eight variables, Des. Codes Cryptogr., 68, 1, 395-406 (2013) · Zbl 1280.94053

[10] Hou, X-D, Classification of self dual quadratic bent functions, Des. Codes Cryptogr., 63, 2, 183-198 (2012) · Zbl 1264.06021

[11] Hyun, Jy; Lee, H.; Lee, Y., MacWilliams duality and Gleason-type theorem on self-dual bent functions, Des. Codes Cryptogr., 63, 3, 295-304 (2012) · Zbl 1259.94071

[12] Janusz, Gj, Parametrization of self-dual codes by orthogonal matrices, Finite Fields Appl., 13, 3, 450-491 (2007) · Zbl 1138.94389

[13] Kolomeec, Na, The graph of minimal distances of bent functions and its properties, Des. Codes Cryptogr., 85, 3, 1-16 (2017) · Zbl 1417.94138

[14] Kutsenko, Av, The Hamming distance spectrum between self-dual Maiorana-McFarland bent functions, J. Appl. Ind. Math., 12, 1, 112-125 (2018) · Zbl 1413.94045

[15] Langevin, P.; Leander, G.; Mcguire, G., Kasami bent function are not equivalent to their duals, Finite Fields Appl., 461, 187-197 (2008) · Zbl 1173.94468

[16] Luo, Gaojun; Cao, Xiwang; Mesnager, Sihem, Several new classes of self-dual bent functions derived from involutions, Cryptography and Communications, 11, 6, 1261-1273 (2019)

[17] Mesnager, S., Several new infinite families of bent functions and their duals, IEEE Trans. Inf. Theory, 60, 7, 4397-4407 (2014) · Zbl 1360.94480

[18] Mesnager, S., Bent Functions: Fundamentals and Results, 544 (2016), Berlin: Springer, Berlin · Zbl 1364.94008

[19] Oblaukhov, Ak, Metric complements to subspaces in the Boolean cube, J. Appl. Ind. Math., 10, 3, 397-403 (2016) · Zbl 1374.94798

[20] Oblaukhov, Ak, A lower bound on the size of the largest metrically regular subset of the Boolean cube, Cryptogr. Commun., 11, 4, 777-791 (2019) · Zbl 1456.94102

[21] Preneel, Bart; Van Leekwijck, Werner; Van Linden, Luc; Govaerts, René; Vandewalle, Joos, Propagation Characteristics of Boolean Functions, Advances in Cryptology — EUROCRYPT '90, 161-173 (1991), Berlin, Heidelberg: Springer Berlin Heidelberg, Berlin, Heidelberg · Zbl 0764.94024

[22] Rothaus, Os, On bent functions, J. Comb. Theory Ser. A, 20, 3, 300-305 (1976) · Zbl 0336.12012

[23] Sok, L.; Shi, M.; Solé, P., Classification and construction of quaternary self-dual bent functions, Cryptogr. Commun., 10, 2, 277-289 (2017) · Zbl 1412.94257

[24] Stănică, P.; Sasao, T.; Butler, Jt, Distance duality on some classes of Boolean functions, J. Comb. Math. Comb. Comput., 107, 181-198 (2018) · Zbl 1432.94228

[25] Tokareva, N., Bent Functions, Results and Applications to Cryptography (2015), London: Academic Press, London · Zbl 1372.94002

[26] Tokareva, Nn, The group of automorphisms of the set of bent functions, Discret. Math. Appl., 20, 5, 655-664 (2010) · Zbl 1211.94057

[27] Tokareva, Nn, On the number of bent functions from iterative constructions: lower bounds and hypotheses, Adv. Math. Commun., 5, 4, 609-621 (2011) · Zbl 1238.94032

[28] Tokareva, N., Duality between bent functions and affine functions, Discret. Math., 312, 666-670 (2012) · Zbl 1234.94068

[29] Wang, Qichun; Johansson, Thomas, A Note on Fast Algebraic Attacks and Higher Order Nonlinearities, Information Security and Cryptology, 404-414 (2011), Berlin, Heidelberg: Springer Berlin Heidelberg, Berlin, Heidelberg · Zbl 1295.94150