zbMATH Open
THE FIRST RESOURCE FOR MATHEMATICS

Kutsenko, A. V.

The Hamming distance spectrum between self-dual Maiorana-McFarland bent functions. (Russian, English) Zbl 1413.94045

Diskretn. Anal. Issled. Oper. 25, No. 1, 98-119 (2018); translation in J. Appl. Ind. Math. 12, No. 1, 112-125 (2018).

Summary: A bent function is self-dual if it is equal to its dual function. We study the metric properties of the self-dual bent functions constructed on using available constructions. We find the full Hamming distance spectrum between self-dual Maiorana-McFarland bent functions. Basing on this, we find the minimal Hamming distance between the functions under study.

MSC:

94A60 Cryptography
94C10 Switching theory, application of Boolean algebra; Boolean functions (MSC2010)
06E30 Boolean functions

Cited in **2** Documents

Keywords:

Hamming distance; self-dual bent function; Maiorana-McFarland bent function

Full Text: DOI

References:

[1] N. A. Kolomeec and A. V. Pavlov, "Properties of Bent Functions with Minimal Distance," Prikl. Diskretn. Mat. No. 4, 5-20 (2009).

[2] O. A. Logachev, A. A. Sal'nikov, S. V. Smyshlyaev, and V. V. Yashchenko, Boolean Functions in Coding Theory and Cryptology (MTsNMO, Moscow, 2012) [in Russian]. · Zbl 1110.94001

[3] F. J. MacWilliams and N. J. A. Sloane, The Theory of Error-Correcting Codes (North-Holland, Amsterdam, 1977; Svyaz',Moscow, 1979). · Zbl 0369.94008

[4] A. K. Oblaukhov, "Metric Complements to Subspaces in the Boolean Cube," Diskretn. Anal. Issled. Oper. 23 (3), 93-106 (2016) [J. Appl. Indust. Math. 10 (3), 397-403 (2016)]. · Zbl 1374.94798

[5] V. N. Potapov, "Cardinality Spectra of Components of Correlation Immune Functions, Bent Functions, Perfect Colorings, and Codes," Probl. Peredachi Inform. 48 (1), 54-63 (2012). [Problems Inform. Transmission 48 (1), 47-55 (2012)]. · Zbl 1276.06008

[6] N. N. Tokareva, "On Decomposition of a Dual Bent Function into Sum of Two Bent Functions," Prikl. Discretn. Mat. No. 4, 59-61 (2014). · Zbl 1325.94143

[7] L. Budaghyan, C. Carlet, T. Helleseth, A. Kholosha, and S. Mesnager, "Further Results on Niho Bent Functions," IEEE Trans. Inform. Theory 58 (11), 6979-6985 (2012). · Zbl 1364.94797

[8] Carlet, C., Boolean Functions for Cryptography and Error-Correcting Codes, 257-397 (2010), New York · Zbl 1209.94035

[9] C. Carlet, L. E. Danielson, M. G. Parker, and P. Solé, "Self-Dual Bent Functions," Int. J. Inform. Coding Theory 1 (4), 384-399 (2010). · Zbl 1204.94118

[10] T.W. Cusick and P. Stănică, Cryptographic Boolean Functions and Applications (Acad. Press, London, 2017). · Zbl 1359.94001

[11] T. Feulner, L. Sok, P. Solé, and A. Wassermann, "Towards the Classification of Self-Dual Bent Functions in Eight Variables," Des. Codes Cryptogr. 68 (1), 395-406 (2013). · Zbl 1280.94053

[12] X.-D. Hou, "On the Coefficients of Binary Bent Functions," Proc. Amer. Math. Soc. 128 (4), 987-996 (2000). · Zbl 0941.94016

[13] X.-D. Hou, "Classification of Self Dual Quadratic Bent Functions," Des. Codes Cryptogr. 63 (2), 183-198 (2012). · Zbl 1264.06021

[14] N. A. Kolomeec, "The Graph of Minimal Distances of Bent Functions and Its Properties," Des. Codes Cryptogr. 85 (3), 1-16 (2017). · Zbl 1417.94138

[15] Kolomeec, N. A.; Pavlov, A. V., Bent Functions on the Minimal Distance, 145-149 (2010), Piscataway

[16] P. Langevin and G. Leander, "Monomial Bent Functions and Stickelberger's Theorem," Finite Fields Appl. 14 (3), 727-742 (2008). · Zbl 1159.11052

[17] R. L. McFarland, "A Family of Difference Sets in Noncyclic Groups," J. Combin. Theory Ser. A, 15 (1), 1-10 (1973). · Zbl

© 2021 FIZ Karlsruhe GmbH

0268.05011

[18] S. Mesnager, "Several New Infinite Families of Bent Functions and Their Duals," IEEE Trans. Inform. Theory 60 (7), 4397-4407 2014). · Zbl 1360.94480

[19] O. Rothaus, "On "Bent" Functions," J.Combin. Theory Ser. A, <Emphasis Type="Bold">20 (3), 300-305 (1976). · Zbl 0336.12012

[20] N. N. Tokareva, "Duality between Bent Functions and Affine Functions," Discrete Math. 312 (3), 666-670 (2012). · Zbl 1234.94068

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

[22] B. Xu, "Dual Bent Functions on Finite Groups and C-Algebras," J. Pure Appl. Algebra 220 (3), 1055-1073 (2016). · Zbl 1327.43004

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.

© 2021 FIZ Karlsruhe GmbH