Canteaut, Anne; **Daum, Magnus**; **Dobbertin, Hans**; **Leander, Gregor**
Finding nonnormal bent functions. (English) Zbl 1091.94021
Discrete Appl. Math. 154, No. 2, 202-218 (2006).

Summary: The question if there exist nonnormal bent functions was an open question for several years. A Boolean function in n variables is called normal if there exists an affine subspace of dimension $n/2$ on which the function is constant. In this paper we give the first nonnormal bent function and even an example for a nonweakly normal bent function. These examples belong to a class of bent functions found in *J.F. Dillon* and *H. Dobbertin* [Finite Fields Appl. 10, No. 3, 342–389 (2004; Zbl 1043.05024)], namely the Kasami functions. We furthermore give a construction which extends these examples to higher dimensions. Additionally, we present a very efficient algorithm that was used to verify the nonnormality of these functions.

MSC:

94A60	Cryptography	Cited in **1** Review
94C10	Switching theory, application of Boolean algebra; Boolean functions (MSC2010)	Cited in **23** Documents
03B70	Logic in computer science	

Keywords:

Algorithm; Boolean function; Bent function; Normal function

Full Text: DOI

References:

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

[2] C. Carlet, Two new classes of bent functions, in: Advances in Cryptology—EUROCRYPT'93, Lecture Notes in Computer Science, vol. 765, Springer, Berlin, 1994, pp. 77-101. · Zbl 0951.94542

[3] Carlet, C., On cryptographic complexity of Boolean functions, (), 53-69 · Zbl 1021.94524

[4] P. Charpin, Normal Boolean functions, J. Complexity 20 (2004) 245-265 (special issue) ("Complexity Issues in Cryptography and Coding Theory", dedicated to Prof. Harald Niederreiter on the occasion of his 60th birthday.)

[5] J.F. Dillon, Elementary hadamard difference sets, Ph.D. Thesis, University of Maryland, USA, 1974. · Zbl 0346.05003

[6] J.F. Dillon, H. Dobbertin, New cyclic difference sets with Singer parameters, Finite Fields Appl. 10 (2004) 342-389. · Zbl 1043.05024

[7] H. Dobbertin, Construction of bent functions and balanced Boolean functions with high nonlinearity, in: Fast Software Encryption—FSE'94, Lecture Notes in Computer Science, vol. 1008, Springer, Berlin, 1995, pp. 61-74. · Zbl 0939.94563

[8] S. Dubuc-Camus, Etude des fonctions booléennes dégénérées et sans corrélation, Ph.D. Thesis, Université de Caen, France, 1998.

[9] B. Preneel, Analysis and design of cryptographic hash functions, Ph.D. Thesis, Katholieke Universiteit Leuven, Belgium, 1993.