**Climent, Joan-Josep**; **García, Francisco J.**; **Requena, Verónica**

**A construction of bent functions of $n+2$ variables from a bent function of $n$ variables and its cyclic shifts.** (English) Zbl 1327.94038

Algebra 2014, Article ID 701298, 11 p. (2014).

Summary: We present a method to iteratively construct new bent functions of $n+2$ variables from a bent function of $n$ variables and its cyclic shift permutations using minterms of $n$ variables and minterms of 2 variables. In addition, we provide the number of bent functions of $n+2$ variables that we can obtain by applying the method here presented, and finally we compare this method with a previous one introduced by us in [*J.-J. Climent* et al., Adv. Math. Commun. 2, No. 4, 421–431 (2008; Zbl 1161.06007)] and with the Rothaus and Maiorana-McFarland constructions.

**MSC:**

94A60 Cryptography
06E30 Boolean functions



**Full Text:** DOI

**References:**

[1] A. Braeken, V. Nikov, S. Nikova, and B. Preneel, "On Boolean functions with generalized cryptographic properties," in Progress in Cryptology-INDOCRYPT 2004, A. Canteaut and K. Viswanathan, Eds., vol. 3348 of Lecture Notes in Computer Science, pp. 120-135, Springer, Berlin, Germany, 2004. · Zbl 1115.94006 · doi:10.1007/b104579

[2] C. Carlet and Y. Tarannikov, "Covering sequences of Boolean functions and their cryptographic significance," Designs, Codes and Cryptography, vol. 25, no. 3, pp. 263-279, 2002. · Zbl 1035.94009 · doi:10.1023/A:1014935513734

[3] K. Kurosawa and R. Matsumoto, "Almost security of cryptographic boolean functions," IEEE Transactions on Information Theory, vol. 50, no. 11, pp. 2752-2761, 2004. · Zbl 1297.94084 · doi:10.1109/TIT.2004.836684

[4] Y. Borissov, A. Braeken, S. Nikova, and B. Preneel, "On the covering radii of binary Reed-Muller codes in the set of resilient boolean functions," IEEE Transactions on Information Theory, vol. 51, no. 3, pp. 1182-1189, 2005. · Zbl 1309.94194 · doi:10.1109/TIT.2004.842779

[5] K. Kurosawa, T. Iwata, and T. Yoshiwara, "New covering radius of Reed-Muller codes for t-resilient functions," IEEE Transactions on Information Theory, vol. 50, no. 3, pp. 468-475, 2004. · Zbl 1288.94067 · doi:10.1109/TIT.2004.824913

[6] C. M. Adams, "Constructing symmetric ciphers using the CAST design procedure," Designs, Codes, and Cryptography, vol. 12, no. 3, pp. 283-316, 1997. · Zbl 0880.94011 · doi:10.1023/A:1008229029587

[7] K. C. Gupta and P. Sarkar, "Improved construction of nonlinear resilient S-boxes," IEEE Transactions on Information Theory, vol. 51, no. 1, pp. 339-348, 2005. · Zbl 1303.94082 · doi:10.1109/TIT.2004.839524/

[8] M. Matsui, "Linear cryptanalysis method for DES cipher," in Advances in Cryptology-EUROCRYPT '93, T. Helleseth, Ed., vol. 765 of Lecture Notes in Computer Science, pp. 386-397, Springer, Berlin, Germany, 1994. · Zbl 0951.94519

[9] K. Nyberg, "Perfect nonlinear S-boxes," in Advances in Cryptology-EUROCRYPT '91, D. W. Davies, Ed., vol. 547 of Lecture Notes in Computer Science, pp. 378-386, Springer, Berlin, Germany, 1991. · Zbl 0766.94012

[10] P. Sarkar and S. Maitra, "Construction of nonlinear Boolean functions with important cryptographic properties," in Advances in Cryptology-EUROCRYPT 2000, B. Preneel, Ed., vol. 1807 of Lecture Notes in Computer Science, pp. 485-506, Springer, Berlin, Germany, 2000. · Zbl 1082.94529

[11] J. Seberry, X.-M. Zhang, and Y. L. Zheng, "Nonlinearity and propagation characteristics of balanced Boolean functions," Information and Computation, vol. 119, no. 1, pp. 1-13, 1995. · Zbl 0832.68040 · doi:10.1006/inco.1995.1073

[12] W. Millan, "How to improve the nonlinearity of bijective S-boxes," in Information Security and Privacy, C. Boyd and E. Dawson, Eds., vol. 1438 of Lecture Notes in Computer Science, pp. 181-192, Springer, Berlin, Germany, 1998. · Zbl 1097.94512

[13] W. Millan, L. Burnet, G. Carter, A. Clark, and E. Dawson, "Evolutionary heuristics for finding cryptographically strong S-boxes," in Information and Communication Security, V. Varadharajan and Y. Mu, Eds., vol. 1726 of Lecture Notes in Computer Science, pp. 263-274, Springer, Berlin, Germany, 1999. · Zbl 1014.94556

[14] J. Detombe and S. Tavares, "Constructing large cryptographically strong S-boxes," in Advances in Cryptology-AUSCRYPT '92, J. Seberry and Y. Zheng, Eds., vol. 718 of Lecture Notes in Computer Science, pp. 165-181, Springer, Berlin, Germany, 1993. · Zbl 0867.94018

[15] C. Carlet, "Two new classes of bent functions," in Advances in Cryptology-EUROCRYPT '93, T. Helleseth, Ed., vol. 765 of Lecture Notes in Computer Science, pp. 77-101, Springer, Berlin, Germany, 1994. · Zbl 0951.94542

[16] C. Carlet, "On the secondary constructions of resilient and bent functions," in Coding, Cryptography and Combinatorics, vol.

23 of Progress in Computer Science and Applied Logic, pp. 3-28, Birkhäuser, Basel, Switzerland, 2004. · Zbl 1062.94036

[17] C. Carlet, "On bent and highly nonlinear balanced/resilient functions and their algebraic immunities," in Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, M. Fossorier, H. Imai, S. Lin, and A. Poli, Eds., vol. 3857 of Lecture Notes in Computer Science, pp. 1-28, Springer, Berlin, Germany, 2006. · Zbl 1125.94014 · doi:10.1007/11617983

[18] C. Carlet, "Boolean functions for cryptography and error-correcting codes," in Boolean Models and Methods in Mathematics, Computer Science, and Engineering, Y. Crama and P. Hammer, Eds., chapter 8, pp. 257-397, Cambridge University Press, New York, NY, USA, 2010. · Zbl 1209.94035

[19] C. Carlet and P. Guillot, "A characterization of binary bent functions," Journal of Combinatorial Theory A, vol. 76, no. 2, pp. 328-335, 1996. · Zbl 0861.94014 · doi:10.1006/jcta.1996.0110

[20] C. Carlet and J. L. Yucas, "Piecewise constructions of bent and almost optimal boolean functions," Designs, Codes, and Cryptography, vol. 37, no. 3, pp. 449-464, 2005. · Zbl 1142.94336 · doi:10.1007/s10623-005-4036-2

[21] D. K. Chang, "Binary bent sequences of order 64," Utilitas Mathematica, vol. 52, pp. 141-151, 1997. · Zbl 0926.94019

[22] J.-J. Climent, F. J. Garćia, and V. Requena, "On the construction of bent functions of n+2 variables from bent functions of n variables," Advances in Mathematics of Communications, vol. 2, no. 4, pp. 421-431, 2008. · Zbl 1161.06007 · doi:10.3934/amc.2008.2.421

[23] T. W. Cusick and P. St\uanic\ua, Cryptographic Boolean Functions and Applications, Academic Press, San Diego, Calif, USA, 2009.

[24] J. F. Dillon, Elementary hadamard difference sets [Ph.D. thesis], University of Maryland, College Park, Md, USA, 1974. · Zbl 0346.05003

[25] H. Dobbertin, "Construction of bent functions and balanced Boolean functions with high nonlinearity," in Fast Sofware Encription, B. Preneel, Ed., vol. 1008 of Lecture Notes in Computer Science, pp. 61-74, Springer, Berlin, Germany, 1995. · Zbl 0939.94563

[26] H. Dobbertin and G. Leander, "Cryptographer's toolkit for construction of 8-bit bent functions," Cryptology ePrint Archive 2005/089, 2005, http://eprint.iacr.org/.

[27] J. Fuller, E. Dawson, and W. Millan, "Evolutionary generation of bent functions for cryptography," in Proceedings of the IEEE Congress on Evolutionary Computation, vol. 2, pp. 1655-1661, December 2003.

[28] X.-D. Hou and P. Langevin, "Results on bent functions," Journal of Combinatorial Theory A, vol. 80, no. 2, pp. 232-246, 1997. · Zbl 0896.05011 · doi:10.1006/jcta.1997.2804

[29] P. V. Kumar, R. A. Scholtz, and L. R. Welch, "Generalized bent functions and their properties," Journal of Combinatorial Theory A, vol. 40, no. 1, pp. 90-107, 1985. · Zbl 0585.94016 · doi:10.1016/0097-3165(85)90049-4

[30] W. Meier and O. Staffelbach, "Nonlinearity criteria for cryptographic functions," in Advances in Cryptology-EUROCRYPT '89, J. J. Quisquater and J. Vandewalle, Eds., vol. 434 of Lecture Notes in Computer Science, pp. 549-562, Springer, Berlin, Germany, 1990. · Zbl 0724.94009

[31] Q. Meng, H. Zhang, J. Cui, and M. Yang, "Almost enumeration of eight-variable bent functions," Cryptology ePrint Archive 2005/100, 2005, http://eprint.iacr.org/.

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

[33] J. Seberry and X. M. Zhang, "Constructions of bent functions from two known bent functions," The Australasian Journal of Combinatorics, vol. 9, pp. 21-35, 1994. · Zbl 0802.05021

[34] N. Tokareva, "On the number of bent functions from iterative constructions: lower bounds and hypothesis," Advances in Mathematics of Communications, vol. 5, no. 4, pp. 609-621, 2011. · Zbl 1238.94032 · doi:10.3934/amc.2011.5.609

[35] N. Y. Yu and G. Gong, "Constructions of quadratic bent functions in polynomial forms," IEEE Transactions on Information Theory, vol. 52, no. 7, pp. 3291-3299, 2006. · Zbl 1297.94113 · doi:10.1109/TIT.2006.876251

[36] R. L. McFarland, "A family of difference sets in noncyclic groups," Journal of Combinatorial Theory A, vol. 15, no. 1, pp. 1-10, 1973. · Zbl 0268.05011 · doi:10.1016/0097-3165(73)90031-9

[37] O. S. Rothaus, "On "bent" functions," Journal of Combinatorial Theory A, vol. 20, no. 3, pp. 300-305, 1976. · Zbl 0766.94012

[38] R. Yarlagadda and J. E. Hershey, "Analysis and synthesis of bent sequences," IEE Proceedings E: Computers and Digital Techniques, vol. 136, no. 2, pp. 112-123, 1989.

[39] C. Charnes, M. Rötteler, and T. Beth, "On homogeneous bent functions," in Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, S. Bozta\cs and I. E. Shparlinski, Eds., vol. 2227 of Lecture Notes in Computer Science, pp. 249-259, Springer, Berlin, Germany, 2001. · Zbl 1057.94017

[40] C. Charnes, M. Rötteler, and T. Beth, "Homogeneous bent functions, invariants, and designs," Designs, Codes and Cryptography, vol. 26, no. 1-3, pp. 139-154, 2002. · Zbl 1026.06015 · doi:10.1023/A:1016509410000

[41] C. Qu, J. Seberry, and J. Pieprzyk, "On the symmetric property of homogeneous Boolean functions," in Information Security and Privacy, J. Pieprzyk, R. Safavi-Naini, and J. Seberry, Eds., vol. 1587 of Lecture Notes in Computer Science, pp. 26-35, Springer, Berlin, Germany, 1999. · Zbl 0919.94019

[42] P. Langevin, "On generalized bent functions," in Eurocode '92, vol. 339 of CISM Courses and Lectures, pp. 147-157, Springer, New York, NY, USA, 1992. · Zbl 0784.94020

[43] A. Canteaut and P. Charpin, "Decomposing bent functions," IEEE Transactions on Information Theory, vol. 49, no. 8, pp. 2004-2019, 2003. · Zbl 1184.94230 · doi:10.1109/TIT.2003.814476

[44] P. Langevin and G. Leander, "Counting all bent functions in dimension eight," in Proceedings of the International Workshop

on Coding and Cryptography, Ullensvang, Norway, May 2009. · Zbl 1215.94059 · doi:10.1007/s10623-010-9455-z

[45] G. D. Cohen, M. G. Karpovsky, H. F. Mattson Jr., and J. R. Schatz, "Covering radius-survey and recent results," IEEE Transactions on Information Theory, vol. 31, no. 3, pp. 328-343, 1985. · Zbl 0586.94014 · doi:10.1109/TIT.1985.1057043

[46] J. Seberry, X.-M. Zhang, and Y. Zheng, "Systematic generation of cryptographically robust S-boxes (extended abstract)," in Proceedings of the 1st ACM Conference on Computer and Communications Security, pp. 171-182, Fairfax, Va, USA, November 1993.

[47] A. Braeken, Y. Borissov, S. Nikova, and B. Preneel, "Classication of Boolean functions of 6 variables or less with respect to some cryptographic properties," in Automata, Languages and Programming, L. Caires, G. F. Italiano, L. Monteiro, C. Palamidessi, and M. Yung, Eds., vol. 3580 of Lecture Notes in Computer Science, pp. 324-334, Springer, Berlin, Germany, 2005. · Zbl 1082.94011 · doi:10.1007/11523468

[48] A. Canteaut, M. Daum, H. Dobbertin, and G. Leander, "Finding nonnormal bent functions," Discrete Applied Mathematics, vol. 154, no. 2, pp. 202-218, 2006. · Zbl 1091.94021 · doi:10.1016/j.dam.2005.03.027

[49] M. Daum, H. Dobbertin, and G. Leander, "An algorithm for checking normality of Boolean functions," in Proceedings of the International Workshop on Coding and Cryptography (WCC '03), pp. 133-142, March 2003.

[50] S. A. Vanstone and P. C. van Oorschot, An Introduction to Error Correcting Codes with Applications, Kluwer Academic, Boston, Mass, USA, 1989. · Zbl 0726.94006