Horadam, K. J.; **Farmer, D. G.**

Bundles, presemifields and nonlinear functions. (English) Zbl 1178.94190

Des. Codes Cryptography 49, No. 1-3, 79-94 (2008).

Summary: Bundles are equivalence classes of functions derived from equivalence classes of transversals. They preserve measures of resistance to differential and linear cryptanalysis. For functions over GF(2^n), affine bundles coincide with EA-equivalence classes. From equivalence classes ("bundles") of presemifields of order p^n, we derive bundles of functions over GF(p^n) of the form $\lambda(x) * \rho(x)$, where λ, ρ are linearised permutation polynomials and $*$ is a presemifield multiplication. We prove there are exactly p bundles of presemifields of order p^2 and give a representative of each. We compute all bundles of presemifields of orders $p^n \leq 27$ and in the isotopism class of GF(32) and we measure the differential uniformity of the derived $\lambda(x) * \rho(x)$. This technique produces functions with low differential uniformity, including PN functions (p odd), and quadratic APN and differentially 4-uniform functions ($p = 2$).

MSC:

94A60 Cryptography
12K10 Semifields
11T71 Algebraic coding theory; cryptography (number-theoretic aspects)
20J06 Cohomology of groups

Software:

Magma

Full Text: DOI

References:

[1] Berger T.P., Canteaut A., Charpin P., Laigle-Chapuy Y. (2006) On almost perfect nonlinear functions over \(\mathbb F_{2^n}\) . IEEE Trans. Inform. Theory 52:4160–4170 · Zbl 1184.94224 · doi:10.1109/TIT.2006.880036

[2] Bosma W., Cannon J., Playoust C. (1997) The MAGMA algebra system I: the user language. J. Symbol. Comp. 24:235–265 · Zbl 0898.68039 · doi:10.1006/jsco.1996.0125

[3] Brinkmann M., Leander G.: On the classification of APN functions up to dimension five. In: Proceedings, International Workshop on Coding and Cryptography, April 16–20, 2007, INRIA-Rocquencourt, France, pp. 39–48 (2007). · Zbl 1184.94227

[4] Budaghyan L., Carlet C., Leander G.: Another class of quadratic APN binomials over \(\mathbb F_{2^n}\) : the case n divisible by 4. In: Proceedings, International Workshop on Coding and Cryptography, April 16–20, 2007, INRIA-Rocquencourt, France, pp. 49–58 (2007).

[5] Budaghyan L., Carlet C., Felke P., Leander G.: An infinite class of quadratic APN functions which are not equivalent to power mappings, Cryptology ePrint Archive: Report 2005/359 http://eprint.iacr.org/2005/35 . In: Proceedings ISIT, July 9–14, 2006, Seattle, USA, IEEE, pp. 2637–2641 (2006).

[6] Budaghyan L., Carlet C., Pott A. (2006) New classes of almost bent and almost perfect nonlinear polynomials. IEEE Trans. Inform. Theory 52:1141–1152 · Zbl 1177.94136 · doi:10.1109/TIT.2005.864481

[7] Carlet C.: Boolean functions for cryptography and error-correcting codes; and, Vectorial Boolean functions for cryptography. In: Hammer P., Crama Y. (eds.) Boolean Methods and Models, CUP, Cambridge (to appear). · Zbl 1209.94035

[8] Carlet C., Charpin P., Zinoviev V. (1998) Codes, bent functions and permutations suitable for DES-like cryptosystems. Des. Codes Cryptogr. 15:125–156 · Zbl 0938.94011 · doi:10.1023/A:1008344232130

[9] Carlet C., Ding C. (2004) Highly nonlinear mappings. J. Complexity 20:205–244 · Zbl 1053.94011 · doi:10.1016/j.jco.2003.08.008

[10] Colbourn C.J., Dinitz J.H. (eds) (1996) The CRC Handbook of Combinatorial Designs. CRC Press, Boca Raton · Zbl 0836.00010

[11] Cordero M., Wene G.P. (1999) A survey of finite semifields. Discrete Math. 208/209:125–137 · Zbl 1031.12009 · doi:10.1016/S0012-365X(99)00068-0

[12] Coulter R.S., Matthews R.W. (1997) Planar functions and planes of Lenz-Barlotti Class II. Des. Codes Cryptogr. 10:167–184 · Zbl 0872.51007 · doi:10.1023/A:1008292303803

[13] Dobbertin H. (1999) Almost perfect nonlinear power functions on GF(2 n): the Welch case. IEEE Trans. Inform. Theory 45:1271–1275 · Zbl 0957.94021 · doi:10.1109/18.761283

[14] Edel Y., Kyureghyan G., Pott A. (2006) A new APN function which is not equivalent to a power mapping. IEEE Trans. Inform. Theory 52:744–747 · Zbl 1246.11185 · doi:10.1109/TIT.2005.862128

[15] Galati J.C. (2004) A group extensions approach to relative difference sets. J. Combin. Designs 12:279–298 · Zbl 1045.05021 · doi:10.1002/jcd.10090

[16] Horadam K.J.: Differential uniformity for arrays, cryptography and coding. In: Proceedings of the 9th IMA International Conference, LNCS 2898, pp. 115–124. Springer, Berlin (2003). · Zbl 1123.94346

[17] Horadam K.J. (2006) A theory of highly nonlinear functions. In: Fossorier M., et al. (eds) AAECC-16, LNCS 3857. Springer, Berlin, pp. 87–100 · Zbl 1125.94022

[18] Horadam K.J. (2007) Hadamard Matrices and Their Applications. Princeton University Press, Princeton, NJ · Zbl 1145.05014

[19] Horadam K.J.: Transversals and graphs: bundles, CCZ and EA equivalence of functions, manuscript in preparation.

[20] Horadam K.J., Farmer D.G.: Bundles, presemifields and nonlinear functions. In: Proceedings, International Workshop on Coding and Cryptography, April 16–20, 2007, INRIA-Rocquencourt, France, pp. 197–206 (2007). · Zbl 1178.94190

[21] Horadam K.J., Udaya P. (2002) A new construction of central relative (p a , p a , p a , 1)-difference sets. Des. Codes Cryptogr. 27:281–295 · Zbl 1027.05013 · doi:10.1023/A:1019999223151

[22] Knuth D.E. (1965) Finite semifields and projective planes. J. Algebra 2:182–217 · Zbl 0128.25604 · doi:10.1016/0021-8693(65)90018-9

[23] Kyureghyan G.M. (2007) Crooked maps in \(\mathbb F_{2^n}\) . Finite Field Appl. 13:713–726 · Zbl 1170.94009 · doi:10.1016/j.ffa.2006.03.003

[24] Leander G., Poschmann A. (2007) On the classification of 4-bit S-boxes. In: Carlet C., Sunar B. (eds) WAIFI 2007, LNCS 4547. Springer, Berlin, pp. 159–176 · Zbl 1184.94239

[25] LeBel A., Horadam K.J.: Direct sums of balanced functions, perfect nonlinear functions and orthogonal cocycles. J. Combin. Designs (2008) to appear. · Zbl 1136.94006

[26] Nakagawa N., Yoshiara S. (2007) A construction of differentially 4-uniform functions from commutative semifields of characteristic 2. In: Carlet C., Sunar B. (eds). WAIFI 2007, LNCS 4547. Springer, Berlin, pp. 134–146 · Zbl 1213.11196

[27] Perera A.A.I., Horadam K.J. (1998) Cocyclic generalised Hadamard matrices and central relative difference sets. Des. Codes Cryptogr. 15:187–200 · Zbl 0919.05007 · doi:10.1023/A:1008367718018

[28] Pott A. (2004) Nonlinear functions in Abelian groups and relative difference sets. Discrete Appl. Math. 138:177–193 · Zbl 1035.05023 · doi:10.1016/S0166-218X(03)00293-2