Budaghyan, Lilya; **Helleseth, Tor**

New commutative semifields defined by new PN multinomials. (English) Zbl 1291.12006

Cryptogr. Commun. 3, No. 1, 1-16 (2011).

Summary: We introduce two infinite classes of quadratic PN multinomials over $\mathbb{F}_{p^{2k}}$ where p is any odd prime. We prove that for k odd one of these classes defines a new family of commutative semifields (in part by studying the nuclei of these semifields). After the works of *L. E. Dickson* [Trans. Am. Math. Soc. 7, 514–522 (1906; JFM 37.0112.01)] and *A. A. Albert* [Trans. Am. Math. Soc. 72, 296–309 (1952; Zbl 0046.03601)], this is the firstly found infinite family of commutative semifields which is defined for all odd primes p. These results also imply that these PN functions are CCZ-inequivalent to all previously known PN mappings.

MSC:

12K10 Semifields
11T71 Algebraic coding theory; cryptography (number-theoretic aspects)
94A60 Cryptography
51E99 Finite geometry and special incidence structures

Keywords:

commutative semifield; equivalence of functions; perfect nonlinear; planar function

Full Text: DOI

References:

[1] Albert, A.A.: On nonassociative division algebras. Trans. Am. Math. Soc. 72, 296–309 (1952) · Zbl 0046.03601 · doi:10.1090/S0002-9947-1952-0047027-4

[2] Biham, E., Shamir, A.: Differential cryptanalysis of DES-like cryptosystems. J. Cryptol. 4(1), 3–72 (1991) · Zbl 0729.68017 · doi:10.1007/BF00630563

[3] Bracken, C., Byrne, E., Markin, N., McGuire, G.: New families of quadratic almost perfect nonlinear trinomials and multinomials. Finite Fields Their Appl. 14(3), 703–714 (2008) · Zbl 1153.11058 · doi:10.1016/j.ffa.2007.11.002

[4] Budaghyan, L., Carlet, C., Pott, A.: New classes of almost bent and almost perfect nonlinear functions. IEEE Trans. Inf. Theory 52(3), 1141–1152 (2006) · Zbl 1177.94136 · doi:10.1109/TIT.2005.864481

[5] Budaghyan, L., Helleseth, T.: New perfect nonlinear multinomials over \$\(\backslash\)textbf\{F\}_\{p\^\{2k\}\}\$ for any odd prime p. In: Proceedings of International Conference on Sequences and Their Applications SETA 2008. Lecture Notes in Computer Science, vol. 5203, pp. 401–414 (2008) · Zbl 1177.94137

[6] Carlet, C., Charpin, P., Zinoviev, V.: Codes, bent functions and permutations suitable for DES-like cryptosystems. Des. Codes Cryptogr. 15(2), 125–156 (1998) · Zbl 0938.94011 · doi:10.1023/A:1008344232130

[7] Coulter, R.S., Matthews R.W.: Planar functions and planes of Lenz–Barlotti class II. Des. Codes Cryptogr. 10, 67–184 (1997) · Zbl 0872.51007

[8] Coulter, R.S., Henderson, M.: Commutative presemifields and semifields. Adv. Math. 217, 282–304 (2008) · Zbl 1194.12007 · doi:10.1016/j.aim.2007.07.007

[9] Dembowski, P., Ostrom, T.: Planes of order n with collineation groups of order n 2. Math. Z. 103, 239–258 (1968) · Zbl 0163.42402 · doi:10.1007/BF01111042

[10] Dickson, L.E.: On commutative linear algebras in which division is always uniquely possible. Trans. Am. Math. Soc 7, 514–522, (1906) · Zbl 37.0112.01 · doi:10.1090/S0002-9947-1906-1500764-6

[11] Dickson, L.E.: Linear algebras with associativity not assumed. Duke Math. J. 1, 113–125 (1935) · Zbl 0012.14801 · doi:10.1215/S0012-7094-35-00112-0

[12] Helleseth, T., Rong, C., Sandberg, D.: New families of almost perfect nonlinear power mappings. IEEE Trans. Inf. Theory 45, 475–485 (1999) · Zbl 0960.11051 · doi:10.1109/18.748997

[13] Helleseth, T., Sandberg, D.: Some power mappings with low differential uniformity. Appl. Algebra Eng. Commun. Comput. 8, 363–370 (1997) · Zbl 0886.11067 · doi:10.1007/s002000050073

[14] Kyureghyan, G., Pott, A.: Some theorems on planar mappings. In: Proceedings of WAIFI 2008. Lecture Notes in Computer Science, vol. 5130, pp. 115–122 (2008) · Zbl 1180.94056

[15] Minami, K., Nakagawa, N.: On planar functions of elementary abelian p-group type. Hokkaido Math. J. 37, 531–544 · Zbl 1161.51003

[16] Ness, G.J.: Correlation of sequences of different lengths and related topics. Ph.D. dissertation, University of Bergen, Norway (2007) · Zbl 1318.94060

[17] Nyberg, K.: Differentially uniform mappings for cryptography. In: Advances in Cryptography, EUROCRYPT'93. LNCS, vol. 765, pp. 55–64 (1994) · Zbl 0951.94510

[18] Zha, Z., Kyureghyan, G., Wang, X.: Perfect nonlinear binomials and their semifields. Finite Fields Their Appl. 15(2), 125–133 (2009) · Zbl 1194.12003 · doi:10.1016/j.ffa.2008.09.002