Li, Yongqiang; **Wang, Mingsheng**

Constructing differentially 4-uniform permutations over $\mathrm{GF}(2^{2m})$ **from quadratic APN permutations over** $\mathrm{GF}(2^{2m+1})$**.** (English) Zbl 1319.94077

Des. Codes Cryptography 72, No. 2, 249-264 (2014).

Summary: In this paper, by means of the idea proposed by *C. Carlet* [ACISP 2011, Lect. Notes Comput. Sci. 6812, 1–15 (2011; Zbl 1279.94060)], differentially 4-uniform permutations with the best known nonlinearity over $\mathbb{F}_{2^{2m}}$ are constructed using quadratic APN permutations over $\mathbb{F}_{2^{2m+1}}$. Special constructions are given using the Gold functions. The algebraic degree of the constructions and their compositional inverses is also investigated. One construction and its compositional inverse both have algebraic degree $m+1$ over $\mathbb{F}_2^{2m}$.

MSC:

94A60 Cryptography
06E30 Boolean functions
11T06 Polynomials over finite fields

Keywords:

permutation; differential uniformity; nonlinearity; algebraic degree

Full Text: DOI

References:

[1] Beth T., Ding C.: On almost perfect nonlinear permutations. In: Advances in Cryptology—EUROCRYPT'93. LNCS, vol. 765, pp. 65-76. Springer, New York (1994). · Zbl 0951.94524

[2] Biham, E.; Shamir, A., Defferential cryptanalysis of DES-like cryptosystems, J. Cryptol., 4, 3-72, (1991) · Zbl 0729.68017

[3] Bracken, C.; Leander, G., A highly nonlinear differentially 4 uniform power mapping that permutes fields of even degree, Finite Fields Appl., 16, 231-242, (2010) · Zbl 1194.94182

[4] Bracken, C.; Byrne, E.; Markin, N.; McGuire, G., New families of quadratic almost perfect nonlinear trinomials and multinomials, Finite Fields Appl., 14, 703-714, (2008) · Zbl 1153.11058

[5] Bracken, C.; Byrne, E.; Markin, N.; McGuire, G., A few more quadratic APN functions, Cryptogr. Commun., 3, 43-53, (2011) · Zbl 1282.11162

[6] Bracken, C.; Tan, C.H.; Tan, Y., Binomial differentially 4 uniform permutations with high nonlinearity, Finite Fields Appl., 18, 537-546, (2012) · Zbl 1267.94043

[7] Browning, K.A.; Dillon, J.F.; Kibler, R.E.; McQuistan, M.T., APN polynomials and related codes, J. Comb. Inf. Syst. Sci., 34, 135-159, (2009) · Zbl 1269.94035

[8] Budaghyan L.: The Simplest Method for Constructing APN Polynomials EA-Inequivalent to Power Functions. WAIFI 2007, LNCS 4547, pp. 177-188. Springer, Heidelberg (2007). · Zbl 1177.94133

[9] Budaghyan, L.; Carlet, C., Classes of quadratic APN trinomials and hexanomials and related structures, IEEE Trans. Inf. Theory, 54, 2354-2357, (2008) · Zbl 1177.94134

[10] Budaghyan, L.; Carlet, C.; Pott, A., New classes of almost bent and almost perfect nonlinear polynomials, IEEE Trans. Inf. Theory, 52, 1141-1152, (2006) · Zbl 1177.94136

[11] Budaghyan, L.; Carlet, C.; Leander, G., Two classes of quadratic APN binomials inequivalent to power functions, IEEE Trans. Inf. Theory, 54, 4218-4229, (2008) · Zbl 1177.94135

[12] Budaghyan, L.; Carlet, C.; Leander, G., Constructing new APN functions from known ones, Finite Fields Appl., 15, 150-159, (2009) · Zbl 1184.94228

[13] Carlet, C.; Crama, Y. (ed.); Hammer, P.L. (ed.), Boolean functions for cryptography and error correcting codes, 257-397, (2010), Cambridge · Zbl 1209.94035

[14] Carlet, C.; Crama, Y. (ed.); Hammer, P.L. (ed.), Vectorial Boolean functions for cryptography, 398-469, (2010), Cambridge · Zbl 1209.94036

[15] Carlet C.: On known and new differentially uniform functions. ACISP 1-15 (2011). · Zbl 1279.94060

[16] Carlet, C.; Charpin, P.; Zinoviev, V., Codes, bent functions and permutations sutiable for DES-like cryptosystems, Des. Codes Cryptogr., 15, 125-156, (1998) · Zbl 0938.94011

[17] Chabaud F., Vaudenay S.: Links between differential and linear cryptanalysis. In: Advances in Cryptology—EUROCRYPT'94. LNCS, vol. 950, pp. 356-365. Springer, New York (1995). · Zbl 0879.94023

[18] Dillon J.F.: APN polynomials: An Update. In: International Conference on Fields and Applications Fq9, Dublin, Ireland (2009). · Zbl 1184.94228

[19] Dobbertin, H., One-to-one highly nonlinear power functions on GF(2\^{}\{n\}), Appl. Algebra Eng. Commun. Comput., 9, 139-152, (1998) · Zbl 0924.94026

[20] Gold, R., Maximal recursive sequences with 3-valued recursive crosscorrelation functions, IEEE Trans. Inf. Theory, 14, 154-156, (1968) · Zbl 0228.62040

[21] Kasami, T., The weight enumerators for several classes of subcodes of the second order binary Reed-muller codes, Inf. Control, 18, 369-394, (1971) · Zbl 0217.58802

[22] Knudsen L.: Truncated and higher order differentials. In: Preneel, B. (ed.) FSE 1994. LNCS, vol. 1008, pp. 196-211. Springer, Heidelberg (1995). · Zbl 0939.94556

[23] Lachaud, G.; Wolfmann, J., The weights of the orthogonals of the extended quadratic binary Goppa codes, IEEE Trans. Inf. Theory, 36, 686-692, (1990) · Zbl 0703.94011

[24] Li, Y.; Wang, M., On EA-equivalence of certain permutations to power mappings, Des. Codes Cryptogr., 58, 259-269, (2011) · Zbl 1216.94049

[25] Li, Y.; Wang, M., Permutation polynomials EA-equivalent to the inverse function over GF(2\^{}\{n\}), Cryptogr. Commun., 3, 175-186, (2011) · Zbl 1251.94032

[26] Matsui M.: Linear cryptanalysis method for DES cipher. In: Advances in Cryptology—EUROCRYPT'93. Lecture Notes in computer Science, vol. 765, pp. 386-397. Springer, New York (1994). · Zbl 0951.94519

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

[28] Nyberg K.: S-boxes and round functions with controllable linearity and differential uniformity. In: Proceedings of Fast Software Encryption 1994. Lecture Notes in Computer Science, vol. 1008, pp. 111-130. Springer, Berlin (1995). · Zbl 0939.94559

[29] Pasalic, E.; Charpin, P., Some results concerning cryptographically significant mappings over GF(2\^{}\{n\}), Des. Codes Cryptogr., 57, 257-269, (2010) · Zbl 1197.94201