Fu, Shihui; **Feng, Xiutao**

Involutory differentially 4-uniform permutations from known constructions. (English)

Zbl 1403.94058
Des. Codes Cryptography 87, No. 1, 31-56 (2019).

Summary: Substitution boxes (S-boxes) are important components of block ciphers that can cause confusion in cryptosystems. The functions used as S-boxes should have low differential uniformity, high nonlinearity and high algebraic degree. When $k > 3$, due to the lack of knowledge about the existence of almost perfect nonlinear permutations over $\mathbb{F}_{2^{2k}}$, which can offer optimal resistance to the differential cryptanalysis, S-boxes are often constructed from differentially 4-uniform permutations. To date, many infinite families of such functions have been constructed. In addition, the lower hardware implementation cost of S-boxes is an important criterion in the design of block ciphers. If the S-box is an involution, which means that the permutation is its own compositional inverse, then the implementation cost for its inverse can be saved. The same hardware circuit can thus be used for both encryption and decryption, which is an advantage in hardware implementation. In this paper, we investigate all of the differentially 4-uniform permutations that are known in the literature and determine whether they can be involutory. We find that some involutory differentially 4-uniform permutations with high nonlinearity and algebraic degree can be given from these known constructions. We also give some partial results and computer experiments to consider the problem of whether a permutation can be affine equivalent to an involution or it will become an involution upon adding an affine function. Some new families of differentially 4-uniform involutions constructed by composing the inverse function and cycles with length 3 are also given. This family of constructions has a high nonlinearity and a maximum algebraic degree.

MSC:

94A60 Cryptography
94C10 Switching theory, application of Boolean algebra; Boolean functions (MSC2010)
14G50 Applications to coding theory and cryptography of arithmetic geometry

Keywords:

involution; differentially 4-uniform permutation; nonlinearity; permutation; algebraic degree

Software:

Midori; PRINCE

Full Text: DOI

References:

[1] Banik S., Bogdanov A., Isobe T., Shibutani K., Hiwatari H., Akishita T., Regazzoni F.: Midori: a block cipher for low energy. In: Advances in Cryptology—ASIACRYPT 2015—21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29-December 3, 2015, Proceedings, Part II, pp. 411-436 (2015). · Zbl 1382.94057

[2] Borghoff J., Canteaut A., Güneysu T., Kavun E.B., Knezevic M., Knudsen L.R., Leander G., Nikov V., Paar C., Rechberger C., Rombouts P., Thomsen S., Yalçin T.: PRINCE—a low-latency block cipher for pervasive computing applications—extended abstract. In: Advances in Cryptology—ASIACRYPT 2012—18th International Conference on the Theory and Application of Cryptology and Information Security, Beijing, China, December 2-6, 2012. Proceedings, pp. 208-225 (2012). · Zbl 1292.94035

[3] Browning K.A., Dillon J.F., McQuistan M.T., Wolfe A.J.: An APN permutation in dimension six. In: Postproceedings of the 9th International Conference on Finite Fields and Their Applications Fq'9. Contemporary Mathematics, vol. 518, pp. 33-42. AMS (2010). · Zbl 1206.94026

[4] Biryukov A.: Analysis of involutional ciphers: Khazad and Anubis. In: 10th International Workshop Fast Software Encryption, FSE 2003, Lund, Sweden, February 24-26, 2003, Revised Papers, pp. 45-53 (2003). · Zbl 1254.94026

[5] 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

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

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

[8] Carlet, C.; Crama, Y. (ed.); Hammer, PL (ed.), Vectorial Boolean functions for cryptography, No. 134, 398-471, (2010), New York

[9] Carlet C.: On known and new differentially uniform functions. In: Proceedings of the 16th Australasian Conference Information Security and Privacy, ACISP 2011, Melbourne, Australia, July 11-13, 2011, pp. 1-15 (2011). · Zbl 1279.94060

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

[11] Canteaut, A.; Duval, S.; Perrin, L., A generalisation of Dillon's APN permutation with the best known differential and nonlinear properties for all fields of size 2^{4k+2}, IEEE Trans. Inf. Theory, 63, 7575-7591, (2017) · Zbl 1390.94813

[12] Chen, X.; Deng, Y.; Zhu, M.; Qu, L., An equivalent condition on the switching construction of differentially 4-uniform permutations on from the inverse function, Int. J. Comput. Math., 94, 1-16, (2016)

[13] Canteaut A., Roué J.: On the behaviors of affine equivalent sboxes regarding differential and linear attacks. In: Proceedings of the 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques Advances in Cryptology (EUROCRYPT 2015), Sofia, Bulgaria, April 26-30, 2015, Part I, pp. 45-74 (2015). · Zbl 1365.94411

[14] Carlet C., Tang D., Tang X., Liao Q.: New construction of differentially 4-uniform bijections. In: Lin D. et al. (eds.) Proceedings of the 9th International Conference on Information Security and Cryptology (Inscrypt 2013), Guangzhou, China, November 27-30, 2013, pp. 22-38. Springer, New York (2014). · Zbl 1347.94024

[15] Chabaud F., Vaudenay S.: Links between differential and linear cryptanalysis. In: Advances in Cryptology—EUROCRYPT'94, Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy, May 9-12, 1994, Proceedings, pp. 356-365 (1994). · Zbl 0879.94023

[16] 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

[17] Fu, S.; Feng, X.; Wu, B., Differentially 4-uniform permutations with the best known nonlinearity from butterflies, IACR Trans. Symmetric Cryptol., 2017, 228-249, (2017)

[18] Grosso V., Leurent G., Standaert F.-X., Varici K., Durvaux F., Gaspar L., Kerckhof S.: SCREAM & iSCREAM side-channel resistant authenticated encryption with masking. Submission to CAESAR, 2014. https://competitions.cr.yp.to/round1/screamv1.pdf.

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

[20] Hirschfeld J.W.P.: Projective Geometries Over Finite Fields, 2nd edn. Oxford Mathematical Monographs, Oxford University Press, Oxford (1998). · Zbl 0899.51002

[21] Kasami, T., The weight enumerators for several classes of subcodes of the 2nd order binary reed-muller codes, Inf. Control, 18, 369-394, (1971) · Zbl 0217.58802

[22] Knudsen L.R.: Truncated and higher order differentials. In: Proceedings of the Second International Workshop on Fast Software Encryption, Leuven, Belgium, 14-16 December 1994, pp. 196-211 (1994).

[23] Kyureghyan G.M.M., Suder V.: On inverses of APN exponents. In: Proceedings of the 2012 IEEE International Symposium on Information Theory, ISIT 2012, Cambridge, MA, USA, July 1-6, 2012, pp. 1207-1211 (2012).

[24] Lai, X.; Blahut, RE (ed.); Costello, DJ (ed.); Maurer, U. (ed.); Mittelholzer, T. (ed.), Higher order derivatives and differential cryptanalysis, No. 276, 227-233, (1994), Boston

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

[26] Li, Y.; Mingsheng, W., Permutation polynomials EA-equivalent to the inverse function over GF(2^n), Cryptogr. Commun., 3, 175-186, (2011) · Zbl 1251.94032

[27] Li, Y.; Wang, M., Constructing differentially 4-uniform permutations over GF(2^{2m}) from quadratic APN permutations over GF(2^{2m+1}), Des. Codes Cryptogr., 72, 249-264, (2014) · Zbl 1319.94077

[28] Li Y., Wang M., Yu Y.: Constructing differentially 4-uniform permutations over GF(2^{2k}) from the inverse function revisited. IACR Cryptology ePrint Archive: Report 2013/731, 2013. https://eprint.iacr.org/2013/731.

[29] Matsui M.: Linear cryptanalysis method for DES cipher. In: Advances in Cryptology—EUROCRYPT'93, Workshop on the Theory and Application of of Cryptographic Techniques, Proceedings, Lofthus, Norway, May 23-27, 1993, pp. 386-397 (1993).

[30] MacWilliams F.J., Sloane N.J.A.: The Theory of Error-correcting Codes. North-Holland Mathematical LibraryNorth-Holland Pub. Co., New York (1977). · Zbl 0369.94008

[31] Nyberg K.: Differentially uniform mappings for cryptography. InL Advances in Cryptology—EUROCRYPT'93, Workshop on the Theory and Application of of Cryptographic Techniques, Proceedings, Lofthus, Norway, May 23-27, 1993, pp. 55-64 (1993).

[32] Peng, J.; Tan, CH, New explicit constructions of differentially 4-uniform permutations via special partitions of $\mathbb{F}_{2^{2k}}$, Finite Fields Appl., 40, 73-89, (2016) · Zbl 1408.94957

[33] Peng, J.; Tan, CH, New differentially 4-uniform permutations by modifying the inverse function on subfields, Cryptogr. Commun., 9, 363-378, (2017) · Zbl 1366.94526

[34] Peng, J.; Tan, CH; Wang, Q., A new family of differentially 4-uniform permutations over $\mathbb{F}_{2^{2k}}$ for odd k, Sci. China Math., 59, 1221-1234, (2016) · Zbl 1354.94044

[35] Perrin L., Udovenko A., Biryukov A.: Cryptanalysis of a theorem: decomposing the only known solution to the big APN

problem. In: Advances in Cryptology—CRYPTO 2016—36th Annual International Cryptology Conference, Proceedings, Santa Barbara, CA, USA, August 14-18, 2016, Part II, pp. 93-122 (2016). · Zbl 1391.94789

[36] Qu, L.; Tan, Y.; Li, C.; Gong, G., More constructions of differentially 4-uniform permutations on $\mathbb{F}_{2^{2k}}$, Des. Codes Cryptogr., 78, 391-408, (2016) · Zbl 1401.94239

[37] Qu, L.; Tan, Y.; Tan, CH; Li, C., Constructing differentially 4-uniform permutations over $\mathbb{F}_{2^{2k}}$ via the switching method, IEEE Trans. Inf. Theory, 59, 4675-4686, (2013) · Zbl 1364.94565

[38] Tang, D.; Carlet, C.; Tang, X., Differentially 4-uniform bijections by permuting the inverse function, Des. Codes Cryptogr., 77, 117-141, (2015) · Zbl 1329.94079

[39] Yuyin, Y.; Wang, M.; Li, Y., Constructing differentially 4 uniform permutations from known ones, Chin. J. Electron., 22, 495-499, (2013)

[40] Zha, Z.; Lei, H.; Sun, S., Constructing new differentially 4-uniform permutations from the inverse function, Finite Fields Appl., 25, 64-78, (2014) · Zbl 1305.94084

[41] Zha, Z.; Lei, H.; Sun, S.; Shan, J., Further results on differentially 4-uniform permutations over $\mathbb{F}_{2^{2m}}$, Sci. China Math., 58, 1577-1588, (2015) · Zbl 1380.94134