zbMATH Open
THE FIRST RESOURCE FOR MATHEMATICS

Charpin, Pascale; **Kyureghyan, Gohar**

When does $G(x) + \gamma \mathbf{Tr}(H(x))$ permute $\mathbb{F}_{p^n}$? (English) Zbl 1229.11153

Finite Fields Appl. 15, No. 5, 615-632 (2009).

The authors examine certain permutation polynomials over finite fields with a focus on linking the nature of such polynomials to their linear structure. The criteria allows to check whether these specified polynomials *fail* to be permutation polynomials.

Reviewer: Richard A. Mollin (Calgary)

MSC:

11T06 Polynomials over finite fields
12E20 Finite fields (field-theoretic aspects)

Cited in **2** Reviews
Cited in **35** Documents

Keywords:

permutation polynomial; linear permutation; p to one mapping; linear structure; linear space; Boolean function

Full Text: DOI

References:

[1] Bierbrauer, J.; Kyureghyan, G., Crooked binomials, Des. codes cryptogr., 46, 269-301, (2008) · Zbl 1196.11162

[2] Budaghyan, L.; Carlet, C.; Leander, G., Constructing new APN from known ones, Finite fields appl., 15, 2, 150-159, (2009) · Zbl 1184.94228

[3] Canteaut, A.; Carlet, C.; Charpin, P.; Fontaine, C., On cryptographic properties of the cosets of $R(1, m)$, IEEE trans. inform. theory, 47, 4, 1494-1513, (2001) · Zbl 1021.94014

[4] Charpin, P.; Kyureghyan, G., On a class of permutation polynomials over $\mathbb{F}_{2^n}$, (), 368-376 · Zbl 1180.11038

[5] Charpin, P.; Pasalic, E., On propagation characteristics of resilient functions, (), 356-365

[6] Charpin, P.; Pasalic, E.; Tavernier, C., On bent and semi-bent quadratic Boolean functions, IEEE trans. inform. theory, 51, 12, 4286-4298, (2005) · Zbl 1184.94234

[7] Dubuc, S., Characterization of linear structures, Des. codes cryptogr., 22, 33-45, (2001) · Zbl 0963.94021

[8] Edel, Y.; Pott, A., A new perfect nonlinear function which is not quadratic, Adv. math. commun., 3, 1, 59-81, (2009) · Zbl 1231.11140

[9] Evertse, J.H., Linear structures in block ciphers, (), 249-266

[10] Hollmann, H.D.L.; Xiang, Q., A class of permutation polynomials of $\mathbb{F}_{2^m}$, Finite fields appl., 11, 1, 111-122, (2005)

[11] Khoo, K.; Gong, G.; Stinson, D.R., A new characterization of semi-bent and bent functions on finite fields, Des. codes cryptogr., 38, 2, 279-295, (2006) · Zbl 1172.11311

[12] Kyureghyan, G., Crooked maps in F_{2^n}, Finite fields appl., 13, 3, 713-726, (2007) · Zbl 1170.94009

[13] Kyureghyan, G., Constructing permutations via linear translators, submitted for publication, available on · Zbl 1241.11136

[14] Kyureghyan, G.; Tan, Y., A family of planar mappings, (), 175-179

[15] Lai, X., Additive and linear structures of cryptographic functions, (), 75-85 · Zbl 0939.94508

[16] Laigle-Chapuy, Y., Permutation polynomials and applications to coding theory, Finite fields appl., 13, 1, 58-70, (2007) · Zbl 1107.11048

[17] Lidl, R.; Niederreiter, H., Finite fields, Encyclopedia math. appl., vol. 20, (1983), Addison-Wesley Reading, MA

[18] McEliece, R.J., Finite fields for computer scientists and engineers, (1987), Kluwer Boston · Zbl 0662.94014

[19] Meier, W.; Staffelbach, O., Nonlinearity criteria for cryptographic functions, (), 549-562

[20] Niederreiter, H.; Robinson, K.H., Complete mappings of finite fields, J. aust. math. soc. ser. A, 33, 197-212, (1982) · Zbl 0495.12018

[21] Patarin, J., Hidden fields equations (HFE) and isomorphisms of polynomials (IP): two new families of asymmetric algorithms, (), 549-562

© 2021 FIZ Karlsruhe GmbH

[22] Yashchenko, V.V., On the propagation criterion for Boolean functions and bent functions, Probl. inf. transm., 33, 1, 62-71, (1997) · Zbl 1037.94560

[23] Yuan, J.; Ding, C.; Wang, H.; Pieprzyk, J., Permutation polynomials of the form $(x^p - x - \delta)^s + L(x)$, Finite fields appl., 14, 4, 482-493, (2008) · Zbl 1211.11136

This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original paper as accurately as possible without claiming the completeness or perfect precision of the matching.

© 2021 FIZ Karlsruhe GmbH