Fu, Shihui; **Feng, Xiutao**; **Lin, Dongdai**; **Wang, Qiang**

A recursive construction of permutation polynomials over $\mathbb{F}_{q^2}$ with odd characteristic related to Rédei functions. (English) Zbl 1445.11141

Des. Codes Cryptography 87, No. 7, 1481-1498 (2019).

Summary: In this paper, we construct two classes of permutation polynomials over $\mathbb{F}_{q^2}$ with odd characteristic closely related to rational Rédei functions. Two distinct characterizations of their compositional inverses are also obtained. These permutation polynomials can be generated recursively. As a consequence, we can generate permutation polynomials with an arbitrary number of terms in a very simple way. Moreover, several classes of permutation binomials and trinomials are given. With the help of a computer, we find that the number of permutation polynomials of these types is quite big.

MSC:

11T06 Polynomials over finite fields

Keywords:

finite fields; permutation polynomials; compositional inverse; Rédei functions; Dickson polynomials

Full Text: DOI

References:

[1] Akbary, A.; Ghioca, D.; Wang, Q., On constructing permutations of finite fields, Finite Fields Appl., 17, 51-67, (2011) · Zbl 1281.11102

[2] Bartoli D., Masuda A.M., Quoos L.: Permutation polynomials over \({\mathbb{F}}_{q^2}\) from rational functions. arXiv:1802.05260 (2018).

[3] Carlet, C.; Ding, C.; Yuan, J., Linear codes from perfect nonlinear mappings and their secret sharing schemes, IEEE Trans. Inf. Theory, 51, 2089-2102, (2005) · Zbl 1192.94114

[4] Ding, C.; Helleseth, T., Optimal ternary cyclic codes from monomials, IEEE Trans. Inf. Theory, 59, 5898-5904, (2013) · Zbl 1364.94652

[5] Ding, C.; Yuan, J., A family of skew Hadamard difference sets, J. Comb. Theory A, 113, 1526-1535, (2006) · Zbl 1106.05016

[6] Ding, C.; Yin, J., Signal sets from functions with optimum nonlinearity, IEEE Trans. Commun., 55, 936-940, (2007)

[7] Ding, C.; Qu, L.; Wang, Q.; Yuan, J.; Yuan, P., Permutation trinomials over finite fields with even characteristic, SIAM J. Discret. Math., 29, 79-92, (2015) · Zbl 1352.11102

[8] Gupta, R.; Sharma, RK, Some new classes of permutation trinomials over finite fields with even characteristic, Finite Fields Appl., 41, 89-96, (2016) · Zbl 1372.11108

[9] Hou, X., Permutation polynomials over finite fields—a survey of recent advances, Finite Fields Appl., 32, 82-119, (2015) · Zbl 1325.11128

[10] Hou, X.; Mullen, GL; Sellers, JA; Yucas, JL, Reversed Dickson polynomials over finite fields, Finite Fields Appl., 15, 748-773, (2009) · Zbl 1228.11174

[11] Laigle-Chapuy, Y., Permutation polynomials and applications to coding theory, Finite Fields Appl., 13, 58-70, (2007) · Zbl 1107.11048

[12] Li N., Helleseth T.: New permutation trinomials from Niho exponents over finite fields with even characteristic. arXiv:1606.03768 (2016). · Zbl 1402.05005

[13] Li, N.; Helleseth, T., Several classes of permutation trinomials from Niho exponents, Cryptogr. Commun., 9, 693-705, (2017) · Zbl 1369.11089

[14] Lidl R., Müller W.B.: Permutation polynomials in RSA-cryptosystems. In: Proceedings of CRYPTO'83 Advances in Cryptology, Santa Barbara, CA, USA, August 21-24, pp. 293-301 (1983).

[15] Lidl R., Mullen G.L., Turnwald G.: Dickson Polynomials. Monographs and Surveys in Pure and Applied Mathematics, vol. 65. Chapman and Hall/CRC, Boca Raton (1993). · Zbl 0823.11070

[16] Lidl R., Niederreiter H.: Finite Fields. Encyclopedia of Mathematica and Its Applications, vol. 20, 2nd edn. Cambridge University Press, Cambridge (1997).

[17] Lee J., Park Y.H.: Some permuting trinomials over finite fields. Acta Math. Sci. Ser. B (English Ed.) \textbf{17}, 250-254,

07 (1997). · Zbl 0921.11062

[18] Li K., Qu L., Li C., Fu S.: New permutation trinomials constructed from fractional polynomials. arXiv:1605.06216 (2016). · Zbl 1402.05004

[19] Li, K.; Qu, L.; Chen, X., New classes of permutation binomials and permutation trinomials over finite fields, Finite Fields Appl., 43, 69-85, (2017) · Zbl 1351.11078

[20] Li, K.; Qu, L.; Chen, X.; Li, C., Permutation polynomials of the form \(cx+\rm Tr_{q^l/q}(x^a)\) and permutation trinomials over finite fields with even characteristic, Cryptogr. Commun., 10, 531-554, (2018) · Zbl 1382.11091

[21] Li K., Qu L., Wang Q.: New constructions of permutation polynomials of the form \(x^rh(x^{q-1})\) over \({\mathbb{F}}_{q^2}\). Des. Codes Cryptogr. (2017). https://doi.org/10.1007/s10623-017-0452-3.

[22] Li K., Qu L., Wang Q.: Compositional inverses of permutation polynomials of the form \(x^rh(x^s)\) over finite fields. Cryptogr. Commun. (2018). https://doi.org/10.1007/s12095-018-0292-7. · Zbl 1409.11125

[23] Mullen G.L., Panario D.: Handbook of Finite Fields. CRC Press, Boca Raton (2013). · Zbl 1319.11001

[24] Niederreiter, H.; Winterhof, A., Cyclotomic R-orthomorphisms of finite fields, Discret. Math., 295, 161-171, (2005) · Zbl 1078.11068

[25] Rivest, RL; Shamir, A.; Adleman, LM, A method for obtaining digital signatures and public-key cryptosystems, Commun. ACM, 21, 120-126, (1978) · Zbl 0368.94005

[26] Schwenk, J.; Huber, K., Public key encryption and digital signatures based on permutation polynomials, Electron. Lett., 34, 759-760, (1998)

[27] Wang Q.: Cyclotomic mapping permutation polynomials over finite fields. In: Sequences, Subsequences, and Consequences, International Workshop, SSC 2007, Los Angeles, CA, USA, May 31-June 2, 2007, Revised Invited Papers, pp. 119-128 (2007). · Zbl 1154.11342

[28] Wang, Q., A note on inverses of cyclotomic mapping permutation polynomials over finite fields, Finite Fields Appl., 45, 422-427, (2017) · Zbl 1404.11138

[29] Yuan, P.; Ding, C., Further results on permutation polynomials over finite fields, Finite Fields Appl., 27, 88-103, (2014) · Zbl 1297.11148

[30] Yuan, P.; Ding, C., Permutation polynomials over finite fields from a powerful lemma, Finite Fields Appl., 17, 560-574, (2011) · Zbl 1258.11100

[31] Yuan, J.; Carlet, C.; Ding, C., The weight distribution of a class of linear codes from perfect nonlinear functions, IEEE Trans. Inf. Theory, 52, 712-717, (2006) · Zbl 1192.94128

[32] Zha, Z.; Hu, L.; Fan, S., Further results on permutation trinomials over finite fields with even characteristic, Finite Fields Appl., 45, 43-52, (2017) · Zbl 1362.05006

[33] Zieve M.: Permutation polynomials on \(\mathbb{F}_q\) induced from bijective Rédei functions on subgroups of the multiplicative group of \(\mathbb{F}_q^*\). arXiv:1310.0776 (2013).

[34] Zieve, ME, On some permutation polynomials over \({\mathbb{F}}_{q}\) of the form \(x^rh(x^{(q-1)/d})\), Proc. Am. Math. Soc., 137, 2209-2216, (2009) · Zbl 1228.11177

[35] Zheng, Y.; Yuan, P.; Pei, D., Large classes of permutation polynomials over \({\mathbb{F}}_{q^2}\), Des. Codes Cryptogr., 81, 505-521, (2016) · Zbl 1396.11139

[36] Zheng, Y.; Yu, Y.; Zhang, Y.; Pei, D., Piecewise constructions of inverses of cyclotomic mapping permutation polynomials, Finite Fields Appl., 40, 1-9, (2016) · Zbl 1364.11154