Xu, Xiaofang; **Feng, Xiutao**; **Zeng, Xiangyong**

Complete permutation polynomials with the form $(x^{p^m}-x+\delta)^s+ax^{p^m}+bx$ over $\mathbb{F}_{p^n}$. (English)

Zbl 1412.11138
Finite Fields Appl. 57, 309-343 (2019).

Summary: In this paper, several classes of complete permutation polynomials with the form $(x^{p^m}-x+\delta)^s+ax^{p^m}+bx$ over $\mathbb{F}_{p^n}$ are proposed by the AGW criterion and determining the number of solutions of some equations. Our results also enrich constructions of known permutation polynomials.

MSC:

11T06 Polynomials over finite fields

Keywords:

complete permutation polynomial; permutation polynomial; AGW criterion; finite field

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.; Giulietti, M.; Zini, G., On monomial complete permutation polynomials, Finite Fields Appl., 41, 132-158, (2016) · Zbl 1372.11107

[3] Bassalygo, L.; Zinoviev, V., Permutation and complete permutation polynomials, Finite Fields Appl., 33, 198-211, (2015) · Zbl 1368.11126

[4] Berlekamp, E. R.; Rumsey, H.; Solomon, G., On the solution of algebraic equations over finite fields, Inf. Control, 10, 6, 553-564, (1967) · Zbl 0166.04803

[5] Feng, D.; Feng, X.; Zhang, W., Loiss: a byte-oriented stream cipher, (IWCC'11 Proceedings of the Third International Conference on Coding and Cryptology, (2011), Springer), 109-125 · Zbl 1272.94029

[6] Gupta, R.; Sharma, R. K., Further results on permutation polynomials of the form $(x^{p^m} - x + \delta)^s + x$ over $\mathbb{F}_{p^{2 m}}$, Finite Fields Appl., 50, 196-208, (2018) · Zbl 1400.11155

[7] Helleseth, T.; Zinoviev, V., New Kloosterman sums identities over $\mathbb{F}_{2^m}$ for all m, Finite Fields Appl., 9, 2, 187-193, (2003) · Zbl 1081.11077

[8] Li, N.; Helleseth, T.; Tang, X., Further results on a class of permutation polynomials over finite fields, Finite Fields Appl., 22, 16-23, (2013) · Zbl 1285.05004

[9] Li, L.; Li, C.; Li, C.; Zeng, X., New classes of complete permutation polynomials, Finite Fields Appl., 55, 177-201, (2019) · Zbl 1401.05016

[10] Li, L.; Wang, S.; Li, C.; Zeng, X., Permutation polynomials $(x^{p^m} - x + \delta)^{s_1} +(x^{p^m} - x + \delta)^{s_2} + x$ over $\mathbb{F}_{p^n}$, Finite Fields Appl., 51, 31-61, (2018) · Zbl 1385.05006

[11] Lidl, R.; Niederreiter, H., Finite Fields, Encycl. Math. Appl., vol. 20, (1997), Cambridge University Press: Cambridge University Press Cambridge

[12] Muratović-Ribić, A.; Pasalic, E., A note on complete polynomials over finite fields and their applications in cryptography, Finite Fields Appl., 25, 306-315, (2014) · Zbl 1302.11096

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

[14] Niederreiter, H.; Robinson, K. H., Complete mappings of finite fields, J. Aust. Math. Soc. A, 33, 2, 197-212, (1982) · Zbl 0495.12018

[15] Niho, Y., Multi-Valued Cross-Correlation Functions Between Two Maximal Linear Recursive Sequences, (1972), University of Southern: University of Southern California, Los Angeles, PhD dissertation

[16] Samardjiska, S.; Gligoroski, D., Quadratic permutation polynomials, complete mappings and mutually orthogonal Latin squares, Math. Slovaca, 67, 5, 1129-1146, (2017) · Zbl 1442.11165

[17] Schnorr, C. P.; Vaudenay, S., Black box cryptanalysis of hash networks based on multipermutations, (Advances in Cryptology-Eurocrypt'94, (1995), Springer), 47-57 · Zbl 0909.94013

[18] Specification of SMS4, block cipher for WLAN products-SMS4, (in Chinese), available at

[19] Stănică, P.; Gangopadhyay, S.; Chaturvedi, A.; Gangopadhyay, A. K.; Maitra, S., Investigations on bent and negabent functions via the negaHadamard transform, IEEE Trans. Inf. Theory, 58, 4064-4072, (2012) · Zbl 1365.94684

[20] Tu, Z.; Zeng, X.; Hu, L., Several classes of complete permutation polynomials, Finite Fields Appl., 25, 182-193, (2014) · Zbl 1284.05012

[21] Tu, Z.; Zeng, X.; Li, C.; Helleseth, T., A classe of new permutation trinomials, Finite Fields Appl., 50, 178-195, (2018) · Zbl 1380.05002

[22] Tu, Z.; Zeng, X.; Jiang, Y., Two classes of permutation polynomials having the form $(x^{2^m} + x + \delta)^s + x$, Finite Fields Appl., 31, 12-24, (2015) · Zbl 1320.11120

[23] Tu, Z.; Zeng, X.; Li, C.; Helleseth, T., Permutation polynomials of the form $(x^{p^m} - x + \delta)^s + L(x)$ over the finite field $\mathbb{F}_{p^{2 m}}$ of odd characteristic, Finite Fields Appl., 34, 20-35, (2015) · Zbl 1315.05008

[24] Tuxanidy, A.; Wang, Q., Compositional inverses and complete mappings over finite fields, Discrete Appl. Math., 217, 318-329, (2017) · Zbl 1372.11111

[25] Wang, L.; Wu, B.; Liu, Z., Further results on permutation polynomials of the form $(x^{p^m} - x + \delta)^s + L(x)$ over $\mathbb{F}_{p^{2 m}}$, Finite Fields Appl., 44, 92-112, (2017) · Zbl 1352.05009

[26] Wang, L.; Wu, B., General constructions of permutation polynomials of the form $(x^{2^m} + x + \delta)^{i(2^m - 1) + 1} + x$ over $\mathbb{F}_{2^{2 m}}$, Finite Fields Appl., 52, 137-155, (2018) · Zbl 1388.05009

[27] Wu, B.; Lin, D., On constructing complete permutation polynomials over finite fields of even characteristic, Discrete Appl. Math., 184, 213-222, (2015) · Zbl 1311.05009

[28] Wu, G.; Li, N.; Helleseth, T.; Zhang, Y., Some classes of monomial complete permutation polynomials over finite fields of characteristic two, Finite Fields Appl., 28, 148-165, (2014) · Zbl 1314.11073

[29] Xu, G.; Cao, X., Complete permutation polynomials over finite fields of odd characteristic, Finite Fields Appl., 31, 228-240, (2015) · Zbl 1320.11121

[30] Xu, X.; Li, C.; Zeng, X.; Helleseth, T., Constructions of complete permutation polynomials, Des. Codes Cryptogr., 86, 12, 2869-2892, (2018) · Zbl 1398.05012

[31] Yuan, J.; Ding, C., Four classes of permutation polynomials of $\mathbb{F}_{2^m}$, Finite Fields Appl., 13, 4, 869-876, (2007) · Zbl 1167.11045

[32] Yuan, J.; Ding, C.; Wang, H.; Pieprzyk, J., Permutation polynomials of the form $(x^p - x + \delta)^s + L(x)$, Finite Fields Appl., 14, 2, 482-493, (2008) · Zbl 1211.11136

[33] Yuan, P.; Zheng, Y., Permutation polynomials from piecewise functions, Finite Fields Appl., 35, 215-230, (2015) · Zbl 1331.11108

[34] Zeng, X.; Zhu, X.; Hu, L., Two new permutation polynomials with the form $(x^{2^k} + x + \delta)^s + x$ over $\mathbb{F}_{2^n}$, Appl. Algebra Eng. Commun. Comput., 21, 2, 145-150, (2010) · Zbl 1215.11116

[35] Zha, Z.; Hu, L., Two classes of permutation polynomials over finite fields, Finite Fields Appl., 18, 4, 781-790, (2012) · Zbl 1288.11111

[36] Zha, Z.; Hu, L., Some classes of permutation polynomials of the form $(x^{p^m} - x + \delta)^s + x$ over $\mathbb{F}_{p^{2 m}}$, Finite Fields Appl., 40, 150-162, (2016) · Zbl 1336.05005

[37] Zha, Z.; Hu, L.; Cao, X., Constructing permutations and complete permutations over finite fields via subfield-valued polynomials, Finite Fields Appl., 31, 162-177, (2015) · Zbl 1320.11123