Fu, Shihui
Two shorter proofs on the inverse and differential spectrum of Bracken-Leander exponent.
(English) Zbl 07414972
Discrete Math. 345, No. 1, Article ID 112658, 7 p. (2022)

Summary: In this paper, we investigate the Bracken-Leander power function $F(x) = x^{2k} + 2^k + 1$ over $\mathbb{F}_{2^{4k}}$ where $k$ is an odd positive integer, and first give a much shorter proof on the binary representation of its inverse based on the Chinese Remainder Theorem. Besides, based on a known connection between the differential spectrum and Fourier spectrum of a function, we also give another shorter proof to determine the differential spectrum of $F(x)$. These two results are solved recently with quite involved skills by L. Kölsch [Des. Codes Cryptography 88, No. 12, 2597–2621 (2020; Zbl 07272718)], M. Xiong and H. Yan [Finite Fields Appl. 48, 117–125 (2017; Zbl 1398.11148)], respectively. We hope that our work is helpful to have a better understanding of this function because of its importance in the construction of S-boxes in block ciphers.

MSC:
11T06 Polynomials over finite fields
14Gxx Arithmetic problems in algebraic geometry; Diophantine geometry
94A60 Cryptography

Keywords:
algebraic degree; Bracken-Leander exponent; compositional inverse; differential spectrum; Fourier spectrum; involution

References:
[1] Blondeau, Céline; Canteaut, Anne; Charpin, Pascale, Differential properties of power functions, Int. J. Inf. Coding Theory, 1, 2, 149-170 (2010) · Zbl 1204.94061

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.