The Multivariate Method strikes again: New Power Mappings with Low Differential Uniformity in odd Characteristic

P. Felke*

*University of Applied Sciences Emden-Leer, Constantiaplatz 4, 26723 Emden,, e-mail: patrick.felke@hs-emden-leer.de

Let \( f(x) = x^d \) be a power mapping over \( \mathbb{F}_{p^n} \) and \( \mathcal{U}_d \) the maximum number of solutions \( x \in \mathbb{F}_{p^n} \) of

\[
f(x + a) - f(x) = b, \quad \text{where } a, b \in \mathbb{F}_{p^n} \text{ and } a \neq 0.
\]

\( f(x) \) is said to be differentially \( k \)-uniform if \( \mathcal{U}_d = k \). This concept is of interest in cryptography, coding theory and communication engineering. The investigation of power functions with low differential uniformity over finite fields \( \mathbb{F}_{p^n} \) of odd characteristic has attracted a lot of research interest since Helleseth, Rong and Sandberg started to conduct extensive computer search to identify such functions. These numerical results are well-known as the Helleseth-Rong-Sandberg tables (see e.g. [1], [3]). From many of their entries infinite families of power mappings \( x^{d_n}, n \in \mathbb{N} \) were extrapolated and their uniformity \( \mathcal{U}_{d_n} \) computed (see e.g. [1], [3], [4], [5], [6]). In [2] the multivariate method introduced by Dobbertin was further developed to compute the uniformity of infinite families of power mappings \( x^{d_n} \) in odd characteristic involving multiplicative characters and Frobenius automorphisms \( X^{p^j} \) of high degree \( p^j \). In this paper we construct new infinite families of power mappings of this kind and prove that their uniformity is low by applying the approach from [2]. In Detail we will prove that for \( x^{d_n}, d_n = \frac{p^n-1}{2} + \frac{p^{n+1}-1}{2} + 1 \) over \( \mathbb{F}_{p^n}, p \geq 7, n \) odd, it is

\[
\mathcal{U}_{d_n} = 3, \text{ if } p \equiv 1 \text{ mod } 4,
\]

\[
\mathcal{U}_{d_n} \in \{2, 4, 6\} \text{ else},
\]

and for \( x^{d_n}, d_n = \frac{3^n-1}{2} + 3^{n+1} - 1 \) over \( \mathbb{F}_3^n, n \) odd, it is \( \mathcal{U}_{d_n} = 4 \). These results explain „open entries“in the Helleseth-Rong-Sandberg tables.

The multivariate method makes use of certain resultants over \( \mathbb{F}_{p^n} \), the so called fundamental polynomials. The application of the multivariate method presented here gives a comprehensive method to compute the uniformity for infinite families of power mappings as above where the corresponding fundamental polynomials can be resolved by certain radicals.

References


