

How to Compute the Low Uniformity of Power Mappings

14th June 2004

Abstract

A power mapping $f(x) = x^d$ is said to be differentially k -uniform if k is the maximum number of solutions $x \in \mathbb{F}_{p^n}$ of $\Delta_d = f(x+1) - f(x) = b, b \in \mathbb{F}_{p^n}$. Computing k and the distribution of Δ_d is of great interest in cryptography and in the theory of sequences. For example the 2-uniform mappings, the so called almost perfect nonlinear (APN) mappings are those, which are maximally immune against differential attacks. Thus the investigation of APN mappings over fields of characteristic 2 has attracted a lot of researchers. APN mappings for odd characteristic have been studied in [2] and [3]. Determining the exact uniformity is a hard problem in general and a systematic approach has not been introduced so far. In this talk we first give a short overview of problems related to computing the k -uniformity of power mappings and describe the multi-variate method introduced in [1] by H. Dobbertin. We apply it to an example from [2] and thereby showing how it can be employed for a systematic study of the distribution of Δ_d and to determine the uniformity of power mappings.

References

- [1] H. Dobbertin: Uniformly representable permutation polynomials, Sequences and their Applications, Proceedings of SETA 01, Springer-Verlag.
- [2] H. Dobbertin, D. Mills, E. N. Müller, A. Pott, W. Willems: APN functions in odd characteristic, Discrete Mathematics 267 (2003), 95-112.
- [3] T. Helleseth, C. Rong, D. Sandberg: New families of almost perfect nonlinear power mappings, IEEE Trans. Inform. Theory 45 (1999) 475-485