Power Mappings with Low Differential Uniformity and Planar Functions

Patrick Felke*

A function $f(x)$ from the field $\mathbb{F}_{p^n}$ to itself is differentially k-uniform if k is the maximum number of solutions $x \in \mathbb{F}_{p^n}$ of $\Delta_{f,a}(x) := f(x+a) - f(x) = b$, where $a, b \in \mathbb{F}_{p^n}$ and $a \neq 0$. Mappings with $k = 1$, i.e. with lowest uniformity possible, are called planar or perfect nonlinear. Planar functions only exist in odd characteristic and were introduced by Dembowski and Ostrom ([5]) to describe projective planes possessing a collineation group with particular properties. We give a survey on recent developments on planar functions and its relation to semifields as given in e.g.[1],[2] or [3]. In [7] Helleseth, Rong and Sandberg gave a table of mappings with low uniformity found by computer search. In [8] they gave a counterexample of the form $X^d, d = \frac{3^n-1}{2} + 2$ to a conjecture due to Dembowski and Ostrom[5] about planar functions. This counterexample has also been discovered by Coulter and Matthews [4]. We discuss the multivariate method, an algebraic framework introduced by Dobbertin and the author (see [6]) to compute the uniformity of certain power mappings and give open problems related to generalized power mappings of the form above involving the quadratic or biquadratic character. Although planar functions posses the best possible resistance against differential cryptanalysis they are not of much interest in cryptography. The proprietary hash function Curl employed in the cryptocurrency IOTA makes use of ternary S-Boxes and is vulnerable to differential cryptanalysis. We believe that Curl and the widely discussed e-mail exchange between MIT media Lab and IOTA foundation might be a good starting point to establish planar functions in cryptography.

References

[1] L. Budaghyan, T. Helleseth: „New perfect nonlinear multinomials over $\mathbb{F}_{p^{2k}}$ for any odd prime p“, in: Proc. of Internat. Conference on Sequences and Their Applications-SETA '08, Lecture Notes in Comput. Sci., Vol. 5203, Springer-Verlag, Berlin, pp. 401-414 (2008).

[2] L. Budaghyan, T. Helleseth: „Planar Functions and Commutative Semifields“, Tatra Mt. Math. Publ. 45 (2010),pp.15-25,doi:10.2478/v10127-010-0002-0

[3] R.S. Coulter, M. Henderson: „Commutative presemifields and semifields“, Adv. Math. 217, pp. 282-304 (2008).

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

[4] R.S. Coulter, R. W. Matthews: „Planar functions and planes of the Lenz-Barlotti class II“. Designs, codes and cryptography 10, pp. 167-184 (1997)

[5] P. Dembowski, T.G. Ostrom: „Planes of order n with collineation groups of order n^2“, Math. Z. 103 (1968), pp. 239-258.

[6] P. Felke: „Computing the Uniformity of Power Mappings. A systematic approach with the multivariate method over finite fields of odd characteristic“, University of Bochum, Germany, 2005

[7] T. Helleseth, C. Rong, D. Sandberg: „New families of almost perfect nonlinear power mappings“, IEEE Trans. Inform. Theory 45 (1999) p. 475-485

[8] T. Helleseth, D.Sandberg: „Some Power Mappings with Low Differential Uniformity“, D. AAECC (1997) 8: 363, pp. 363-370 https://doi.org/10.1007/s002000050073