Cryptology ePrint Archive: Report 2011/627

A note on semi-bent functions with multiple trace terms and hyperelliptic curves

Sihem Mesnager

Abstract: Semi-bent functions with even number of variables are a class of important Boolean functions whose Hadamard transform takes three values. In this note we are interested in the property of semi-bentness of Boolean functions defined on the Galois field F_{2^n} (n even) with multiple trace terms obtained via Niho functions and two Dillon-like functions (the first one has been studied by Mesnager and the second one have been studied very recently by Wang, Tang, Qi, Yang and Xu). We subsequently give a connection between the property of semi-bentness and the number of rational points on some associated hyperelliptic curves. We use the hyperelliptic curve formalism to reduce the computational complexity in order to provide a polynomial time and space test leading to an efficient characterization of semi-bentness of such functions (which includes an efficient characterization of the hyperbent functions proposed by Wang et al.). The idea of this approach goes back to the recent work of Lisonek on the hyperbent functions studied by Charpin and Gong.

Category / Keywords: Boolean function, Walsh-Hadamard transformation, Semi-bent functions, Dickson polynomial, Hyperelliptic curves

Date: received 20 Nov 2011, last revised 28 Nov 2011

Contact author: smesnager at univ-paris8 fr

Available formats: PDF | BibTeX Citation

Version: 20111128:113451 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]