Hyperbent functions

Pascale Charpin[1]

Hyperbent functions were introduced by Youssef and Gong (Eurocrypt 2001). A Boolean bent function f, on $\mathbf{F}_{2^n}$, is said to be hyperbent if it is such that $f(x^k)$ is bent for any k coprime with 2^n-1. Actually, the first definition of hyperbent functions was based on a property of the so-called *extended Hadamard transform* of f which was introduced by Golomb and Gong in *IEEE Trans. Inform. Theory*, 1999. In this paper, the authors proposed that S-boxes should not be approximated by a bijective monomial, providing a new criterion for the S-box design. In their paper Youssef and Gong proposed a large class of possible hyperbent function.

Further, an extensive study of hyperbent functions was made by Carlet and Gaborit (JCT-A, 2006). They established that hyperbent functions can be seen as some codewords of a cyclic code fully characterized by its non zeroes. However, the classification of hyperbent functions is not achieved and many problems remain open. In particular, it seems difficult to define precisely an infinite class of hyperbent functions.

Our recent work, a joint work with Guang Gong[2], has to be placed in this last context. Our purpose is to introduce new tools for the description of hyperbent functions[3].

Monomial hyperbent functions are famous bent functions due to Dillon (1974), who showed that they are strongly related with Kloosterman sums. We solve a problem concerning monomial hyperbent functions which was proposed by Dillon to the second author several years ago.

In the general case we show that the spectrum of a large class of Boolean functions, possibly hyperbent, can be described by means of Dickson polynomials. We further apply this result to a class of binomial functions and to the monomials, providing surprising results.

[1] INRIA, B.P. 105, 78153 Le Chesnay Cedex, France, Pascale.Charpin@inria.fr

[2] Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario, N2L3G1, CANADA, ggong@calliope.uwaterloo.ca

[3] "Hyperbent functions, Kloosterman sums and Dickson polynomials", submitted and research report of the *Center for Applied Cryptographic Research* at University of Waterloo, CACR 2007-29.