Carlet, Claude; **Charpin, Pascale**; **Zinoviev, Victor**

Codes, bent functions and permutations suitable for DES-like cryptosystems. (English)

Zbl 0938.94011
Des. Codes Cryptography 15, No. 2, 125-156 (1998).

Almost bent (AB) and almost perfect nonlinear (APN) functions from $\{0,1\}^m$ to itself are of importance in several topics in information theory, such as with sequences, correlation-immune and resilient functions, permutations for block ciphers, and for resistance against linear and differential cryptanalysis.

After presenting the basic properties of AB functions, the authors develop the coding-theoretic point of view. To this end, they consider a function F from GF(2^m) to itself with $F(0) = 0$, and relate its properties to the properties of the binary code C_F with parity check matrix

$$\begin{bmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ F(1) & F(\alpha) & F(\alpha^2) & \dots & F(\alpha^{n-1}) \end{bmatrix},$$

where $n = 2^m - 1$ and α is primitive in GF(2^m).

Properties of the code C_F are related to F being AB or APN. Results in coding theory due to Kasami give rise to the only known class of AB functions.

The subject of the paper has recently attracted quite some attention is research. Below are some recent references:

H. Dobbertin, "One-to-one highly nonlinear power functions on GF(2^n)", Appl. Algebra Eng. Commun. Comput. 9, 139–152 (1998; Zbl 0924.94026); "Almost perfect nonlinear power functions on GF(2^n): The Niho case", Inf. Comput. 151, 57–72 (1999; Zbl 1072.94513); "Almost perfect nonlinear power functions on GF(2^n): The Welch case", IEEE Trans. Inf. Theory. 45, 1271–1275 (1999; Zbl 0957.94021); *H. D. L. Hollmann* and *Q. Xiang*, "A proof of the Welch and Niho conjectures on cross-correlations of binary m-sequences", Finite Fields Appl. 7, No. 2, 253–286 (2001; Zbl 1027.94006).

Reviewer: L. M. G. M. Tolhuizen (Eindhoven)

MSC:

94A60	Cryptography
11T71	Algebraic coding theory; cryptography (number-theoretic aspects)
94C10	Switching theory, application of Boolean algebra; Boolean functions (MSC2010)
94B05	Linear codes, general
94B15	Cyclic codes

Keywords:

cyclic code; almost bent functions; almost perfect nonlinear functions

Full Text: DOI