Dubuc, Sylvie

Characterization of linear structures. (English) Zbl 0963.94021

Des. Codes Cryptography 22, No. 1, 33-45 (2001).

Let F be a function defined from F_2^m to F_2^n and (α, a) be an element of $F_2^m \times F_2^n$, with $\alpha \neq 0$. Then (α, a) is defined to be a linear structure of F if $F(x) = F(x + \alpha) + a$ for all $x \in F_2^m$.

In this paper the existence of linear structures for F is characterized using the Fourier transform of the function. In particular the case of Boolean functions, i.e. where $n = 1$ is carefully studied. For cryptographic applications Boolean functions without linear structures are desirable. Two constructions of resilient (i.e., correlation-immune and balanced) Boolean functions which have no linear structure are presented.

Reviewer: T.Helleseth (Bergen)

MSC:

94A60 Cryptography
11T71 Algebraic coding theory; cryptography (number-theoretic aspects)

Keywords:

linear structure; Boolean function; vectorial function; Fourier transform

Full Text: DOI