Canteaut, Anne; Charpin, Pascale; Videau, Marion

Cryptanalysis of block ciphers and weight divisibility of some binary codes. (English)

Zbl 1072.94006

Blaum, Mario (ed.) et al., Information, coding and mathematics. Proceedings of workshop honoring Professor Bob McEliece on his 60th birthday, Pasadena, CA, USA, May 24–25, 2002. Boston, MA: Kluwer Academic Publishers (ISBN 1-4020-7079-9/hbk). The Kluwer International Series in Engineering and Computer Science 687, 75-97 (2002).

The security of an iterative block cipher can be defined by some mathematical properties of its round function, and more precisely, by the properties of the confusion function, which is the non linear part of the round function. The authors exploit the fact that such a function F from $\mathbb{F}_2^m$ into $\mathbb{F}_2^m$ can be associated with a binary $[2^m-1, 2m]$ code $\mathcal{C}_F$. The weight divisibility of $\mathcal{C}_F$ (and *R. J. McEliece*'s theorem concerning it [Discrete Math. 3, 177–192 (1972; Zbl 0251.94008)]) provide a powerful tool for evaluating the resistance to linear and high-order differential attacks. The methods used are also based on [Des. Codes Cryptography 15, No. 2, 125–156 (1998; Zbl 0938.94011)]. Also, the authors derive a new upper bound for the degree of some composed functions. At the end of the paper they list the requirements, known up to now, a confusion function must verify to ensure the security and set as an open problem the task of finding all such functions.

For the entire collection see [Zbl 1054.94001].

Reviewer: Nikolai L. Manev (Sofia)

MSC:

94A60	Cryptography
94B15	Cyclic codes
06E30	Boolean functions
94-06	Proceedings, conferences, collections, etc. pertaining to information and communication theory

Cited in **2** Documents

Keywords:

block ciphers; cryptanalysis; almost bent functions; cyclic codes; Boolean functions