Li, Nian; Mesnager, Sihem
Recent results and problems on constructions of linear codes from cryptographic functions.

Summary: Linear codes have a wide range of applications in the data storage systems, communication systems, consumer electronics products since their algebraic structure can be analyzed and they are easy to implement in hardware. How to construct linear codes with excellent properties to meet the demands of practical systems becomes a research topic, and it is an efficient way to construct linear codes from cryptographic functions. In this paper, we will introduce some methods to construct linear codes by using cryptographic functions over finite fields and present some recent results and problems in this area.

MSC:
94B05 Linear codes (general theory)
94D10 Boolean functions
11T71 Algebraic coding theory; cryptography (number-theoretic aspects)

Keywords:
bent function; linear code; perfect nonlinear function; plateaued function

Full Text: DOI

References:

[87] Yang, S.; Yao, Z., Complete weight enumerators of a family of three-weight linear codes, Des Codes Cryptogr., 82, 3, 663-674 (2017) · Zbl 1370.94578


[96] Zhou, Z.; Li, N.; Fan, C.; Helleseth, T., Linear codes with two or three weights from quadratic bent functions, Des Codes Cryptogr., 81, 2, 283-295 (2016) · Zbl 1345.94116


This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original paper as accurately as possible without claiming the completeness or perfect precision of the matching.