Boumezbeur, M.; Mesnager, S.; Guenda, K.
Linear codes from vectorial Boolean functions in the context of algebraic attacks. (English)

MSC:
94B05 Linear codes (general theory)
94D10 Boolean functions
94B15 Cyclic codes
11T71 Algebraic coding theory; cryptography (number-theoretic aspects)
94A60 Cryptography

Keywords:
algebraic attacks; vectorial functions; algebraic immunity; annihilators; cyclic codes; LCD codes; weight distribution

Full Text: DOI

References:
[8] Courtois, N. and Meier, W., Algebraic attacks on stream ciphers with linear feedback, Advances in Cryptology (EUROCRYPT 2003), pp. 345-359. · Zbl 1038.94525


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.