Zhou, Yuhui; Han, Yuhui; Ding, Yang

On the $k$-error linear complexity of sequences from function fields. (English) Zbl 1458.94208


Summary: The linear complexity and the error linear complexity are two important security measures for stream ciphers. We construct periodic sequences from function fields and show that the error linear complexity of these periodic sequences is large. We also give a lower bound for the error linear complexity of a class of nonperiodic sequences.

MSC: 94A55

Keywords: sequence; linear complexity; error linear complexity; algebraic function fields; local expansion

Full Text: DOI

References:


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.