Abstract

The joint linear complexity and k-error joint linear complexity of an m fold 2n periodic multisequence can be efficiently computed using Modified Games Chan algorithm and Extended Stamp Martin Algorithm respectively. In this paper we derived an algorithm for finding the joint linear complexity of a periodic binary multisequence with the help of Modified Games Chan algorithm. Here we derived the minimum value of k for which k-error joint linear complexity is strictly less than the joint linear complexity of binary m fold multisequences of period 2n and an algorithm which, given a constant c and an m fold 2n periodic binary multisequence S, computes the minimum number k of errors and the associated error multisequence needed over a period of S for bringing the joint linear complexity of S below c.

References

Linear Complexity Measures of Binary Multisequences

561, Springer Verlag, 1991
Linear Complexity Measures of Binary Multisequences

Index Terms
Computer Science
Security

Keywords
Word based stream ciphers multisequences error multisequence joint linear complexity k-error joint linear complexity kmin