A note on the (in)security of a stream cipher based on Gopala-Hemachandra Codes

L. Childers, K. Gopalakrishnan*, East Carolina University

We investigate a stream cipher recently proposed in a paper by Nalli and Ozyilmaz which utilizes Gopala-Hemachandra codes. Gopala-Hemachandra codes are derived from Gopala-Hemachandra sequences which are a generalization of the standard Fibonacci Sequence. The cipher was found to have a relatively small keyspace, and moreover, very few keys tend to be valid for a given ciphertext. As a result, we are able to cryptanalyze the ciphertext and recover the plaintext in a fraction of a second for relatively large ciphertexts.

Keywords: Cryptanalysis, Stream Ciphers, Gopala-Hemachandra codes, Fibonacci Codes.