CONFIRMATORY TESTS USED IN CIPHER SYSTEMS EVALUATIONS

Vasile PREDA
University of Bucharest
Academiei Street no.14,
Bucharest, Romania

Emil SIMION
Advanced Technologies Institute
Dinu Vintila Street no.10, S-2
Bucharest, Romania
e-mail:simion@pro.math.unibuc.ro

ABSTRACT.

Linear complexity of a sequence is the size of the shortest feedback shift register which generates the sequence. A method of estimating this complexity consists in successive processing of the sequence and obtaining a monotone increasing sequence of estimators (linear complexity profile) which limit is the linear complexity. The presented results have applications in cryptography, more exactly, they can be used to find the linear equivalent complexity of a cipher algorithm and thus to estimate the cryptographic resistance. In this paper we present some efficient methods of estimating and evaluation the linear equivalent complexity of a cipher algorithm. There are presented some interesting and new results concerning the complexity of the combinations of linear feedback shift registers. These combination can be described in terms of boolean function theory using the logical operators like sum and product. There are also introduced the notion of spliting (a generalization of classical term of decimation) and the inverse operator called interleave. The proofs of the theorems are also given. This work can be easy generalized to quadratic complexity of high order complexity.