CODE WORD ENTROPY

BY

VALERIU MUNTEANU and DANIELA TĂRNICERIU

Unlike the classical entropy used to characterize the code word set, which depends on probabilities only, new entropy, which depends on both probabilities and code word lengths, is defined. The extremum of this entropy is also established. A special case of this entropy, which measures the code redundancy, is analysed.

MINIMIZING CORRELATIONS IN ENCRYPTED DATA STREAMS

BY

LUMINIŢA SCRIPCARIU and PETRUŢ DUMA

Data confidentiality and information secrecy are ensured by encryption techniques which must be sufficiently robust against different cryptographic attacks (differential, linear or brute force) [1]. Most of them are based on the correlation properties of the original file or the correlation between the plaintext and the cipher text. Therefore minimizing these correlations is imperative to design better encryption algorithms, more robust and more efficient. We analyse some well-known algorithms [2] and ours [3], [4], based on invertible functions defined on Galois Fields, with different data structures [5]. Finally a comparison of the correlation values obtained in these cases is made in order to deduce the most efficient encryption methods.

TRANSMISSION LINES AS SOURCE OF INDUSTRIAL FREQUENCY ELECTROMAGNETIC FIELD RADIATION AND A DEVICE FOR ITS ACTIVE SUPPRESSION

BY

LILIANA VORNICU

Transmission lines are a source of electromagnetic field (EMF) in the wide space and affect many electronic devices. It is also known that the influence of the electromagnetic field is harmful to the health of humans. In the present paper it is shown that active suppression of EMF from a transmission line can be achieved by the use of a long loop fed by a controlled current. The loop is placed lengthways on the transmission line, or nearly, in a protected area. The parameters of the loop and the exact place of its arrangement are defined by calculation, and the current in the loop is set by an automatic system.