CORR 2001-55

A Decoding Algorithm for General Linear Block Codes

Abdulrahman Kh. Al Jabri*

Abstract This report introduces a new decoding algorithm for general linear block codes. The algorithm generates a direct estimate of the error locations based on exploiting the statistical information embedded in the classical syndrome decoding. The algorithm can be used to cryptanalyse many algebraic-code public-key, identification and stream cipher cryptosystems. In particular, the algorithm is used to cryptanalyse McEliece public-key cryptosystem where it is shown that the system with its original parameters is not secure.

Keywords Decoding, General Linear Block Codes, McEliece System, Statistical.