Towards a design procedure for cryptosecure substitution boxes

J. A. Gordon

The Hatfield Polytechnic
England

Abstract

Substitution tables (s-boxes) are well known in cryptographic circles, but little seems to have been published regarding design procedures for them. This paper addresses itself to a theoretical examination of the linearity properties of random, reversible s-boxes, i.e. tables of the numbers 0 thru (2^M)-1 in a random order. Bounds on the probabilities of occurrence of various bit-linearities and partial bit-linearities are derived. It is shown that the probability of bit linearity approaches zero rapidly with increasing m. Thus the probability that with M=4, one or more contents bit are a linear function of the address bits is less than about 10E-2. while when M=8 the bound is about 10E-71.

These results could provide part of the answer to the problem of s-box design.