Journal of Systems Science and Complexity 1991 4 (2): 104-110 ISSN: 1000-0577 CN: 11-2019/O1

论文

A CRYPTOGRAPHIC STUDY ON S—BOXES OF DES TYPE Ⅰ AN INTEGRATED ANALYSIS OF THE DESIGN CRITERIA FOR S-BOXES

Yang Junhui(1),Dai Zongduo(2),Zeng Kencheng(3)

(1)Computing Center,Academia Sinica,Beijing 100080,China;(2)Graduate School,Academia Sinica,Beijing 100039,China;(3)Graduate School,Academia Sinica,Beijing 100039,China

收稿日期 修回日期 网络版发布日期 接受日期

摘要 An integrated analysis of the design criteria for the S-boxes used in the DES is made. Among others, the exclusion principle between the degree of nonlinearity and the degree of I/O—correlation immunity for partial variables is established.

关键词 DES,S-box

分类号

A CRYPTOGRAPHIC STUDY ON S—BOXES OF DES TYPE Ⅰ AN INTEGRATED ANALYSIS OF THE DESIGN CRITERIA FOR S-BOXES

Yang Junhui(1),Dai Zongduo(2),Zeng Kencheng(3)

(1)Computing Center,Academia Sinica,Beijing 100080,China;(2)Graduate School,Academia Sinica,Beijing 100039,China;(3)Graduate School,Academia Sinica,Beijing 100039,China

Abstract An integrated analysis of the design criteria for the S-boxes used in the DES is made. Among others, the exclusion principle between the degree of nonlinearity and the degree of I/O—correlation immunity for partial variables is established.

Key words DES S-box

DOI:

通讯作者