计算机工程　2008 34 (5): 158-160　ISSN: 1000-3428　CN: 31-1289/TP

安全技术

SMS4算法S盒的密码学性质

刘 佳1,2，韦宝典1,2，戴宪华1

（1. 中山大学电子与通信工程系，广州 510275；2. 广东省信息安全技术重点实验室，广州 510275）

收稿日期　修回日期　网络版发布日期 2008-2-29　接受日期

摘要　S盒是分组密码的重要组成部分，在很大程度上决定了分组密码的安全性。该文研究了中国分组密码标准SMS4算法S盒的平衡性、差分性质、线性结构、非线性、Walsh谱等性质，通过与美国高级加密标准、欧洲分组加密标准Camellia的S盒作比较，说明了SMS4算法S盒一些较好的安全特性。

关键词　SMS4算法；高级加密标准；S盒；布尔函数

分类号　TP301.6

DOI:

对应的英文版文章：05-62

通讯作者:

作者个人主页: 刘 佳1;2;韦宝典1;2;戴宪华1