计算机工程 2010 36 (1): 154-156,160 ISSN: 1000-3428 CN: 31-1289/TP 首页 当期目录 上一期

安全技术

# 分组密码统一描述模型研究

师国栋，康 绯，顾海文

(解放军信息工程大学信息工程学院，郑州 450002)

收稿日期 修回日期 网络版发布日期 接受日期

摘要 介绍分组密码统一描述模型建立的背景和现实可行性，通过对现有大量分组密码算法结构的研究，对算法各个部分的功能进行归纳，提取分组密码算法的多个通用组件，给出从2种不同角度建立的分组密码统一描述模型——模型的组件关系形式和分组密码流程形式，并对各个通用组件进行了定义和功能说明，应用该模型描述Camellia算法。

关键词

分组密码；统一描述模型；Feistel结构；S盒

分类号 TP309

**DOI:**

通讯作者:

作者个人主页: 师国栋;康 绯;顾海文

扩展功能

本文信息

Supporting info

PDF(315KB)

[HTML全文](0KB)

参考文献[PDF]

参考文献

服务与反馈

把本文推荐给朋友

加入我的书架

加入引用管理器

引用本文

Email Alert

文章反馈

浏览反馈信息

相关信息

本刊中 包含“分组密码；统一描述模型；Feistel结构；S盒”的 相关文章

本文作者相关文章