

<<分组密码的设计与分析>>

图书基本信息

书名：<<分组密码的设计与分析>>

13位ISBN编号：9787302039860

10位ISBN编号：7302039860

出版时间：2000-9-1

出版时间：清华大学出版社

作者：冯登国,吴文玲

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

<<分组密码的设计与分析>>

内容概要

本书主要介绍了设计和分析分组密码的理论和技術，包括现有的有代表性的分组密码及其攻击方法，评测S-盒的安全性能的准则及准则之间的关系，构造安全性能好的S-盒的方法，最新公布的AES候选算法及其分析。

本书是作者在长期从事科研和教学实践的基础上完成的，内容新颖，系统性强，深入浅出，易于理解。

本书可作为计算机专业、通信专业、信息安全专业的硕士生、博士生和本科高

<<分组密码的设计与分析>>

书籍目录

第1章 绪论

1.1 分组密码的研究背景与意义

.....

第2章 典型分组密码简介

2.1 分组密码的数学模型

.....

第3章 分组密码的分析方法

3.1 强力攻击

.....

第4章 分组密码的设计原理

4.1 分组密码的一般设计原理

.....

第5章 分组密码的统计测试原理与密钥管理

5.1 预备知识

.....

第6章 AES候选算法及其分析

6.1 AES的评估准则

.....

参考文献

<<分组密码的设计与分析>>

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>