<<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：9787302204602

10位ISBN编号：7302204608

出版时间：2009-10

出版时间：清华大学出版社

作者：吴文玲，冯登国，张文涛　编著

页数：448

前言

信息安全已成为国家安全的重要组成部分，也是保障信息社会和信息技术可持续发展的核心基础。
信息技术的迅猛发展和深度应用必将带来更多难以解决的信息安全问题，只有掌握了信息安全的科学发展规律，才有可能解决人类社会遇到的各种信息安全问题。
但科学规律的掌握非一朝一夕之功，治水、训火、利用核能曾经都经历了多么漫长的岁月。
无数事实证明，人类是有能力发现规律和认识真理的。
今天对信息安全的认识，就经历了一个从保密到保护，又发展到保障的趋于真理的发展过程。
信息安全是动态发展的，只有相对安全没有绝对安全，任何人都不能宣称自己对信息安全的认识达到终极。
国内外学者已出版了大量的信息安全著作，我和我所领导的团队近10年来也出版了一批信息安全著作，目的是不断提升对信息安全的认识水平。
我相信有了这些基础和积累，一定能够推出更高质量和更高认识水平的信息安全著作，也必将为推动我国信息安全理论与技术的创新研究做出实质性贡献。
本丛书的目标是推出系列具有特色和创新的信息安全理论与技术著作，我们的原则是成熟一本出版一本，不求数量，只求质量。
希望每一本书都能提升读者对相关领域的认识水平，也希望每一本书都能成为经典范本。
我非常感谢清华大学出版社给我们提供了这样一个大舞台，使我们能够实施我们的计划和理想，我也特别感谢清华大学出版社张民老师的支持和帮助。
限于作者的水平，本丛书难免存在不足之处，敬请读者批评指正。

<<分组密码的设计与分析>>

内容概要

本书系统地介绍分组密码的分析方法、设计理论、密钥管理、工作模式和检测评估。
全书共分6篇。
第1篇重点介绍典型分组密码算法以及它们的研究现状。
第2篇系统地讲述分组密码的分析方法，介绍每种分析方法的基本原理以及对典型分组密码的分析示例。
第3篇从整体结构、基础模块、伪随机性等各个方面系统地讲述分组密码的设计理论。
第4篇简单介绍分组密码的密钥管理。
第5篇系统地讲述分组密码工作模式的各种安全模型，同时介绍有代表性的工作模式以及它们的安全性。
第6篇简单介绍分组密码的检测原理和评估要素。
本书可作为密码学专业、信息安全专业、通信专业、计算机专业的硕士生、博士生和本科高年级学生的相关课程的教科书，也可以作为从事相关专业的教学、科研和工程技术人员的参考书。

<<分组密码的设计与分析>>

书籍目录

章节摘录

差分密码分析是一种选择明文攻击，线性密码分析是一种已知明文攻击，用这两种分析方法攻击一个分组密码时，目标是恢复出种子密钥的全部或部分信息。
与这两种分析方法有所不同，相关密钥密码分析赋予了攻击者更多的权限，攻击者虽然不知道密钥值本身，但假设他已知（或可以选择）密钥之间的关系。
本章首先介绍相关密钥密码分析的攻击假设；然后以LoKI89密码为例介绍相关密钥攻击；最后以AES一192为例介绍相关密钥一矩阵攻击、相关密钥一不可能差分攻击和相关密钥一差分线性攻击。
6.1 相关密钥密码分析的攻击假设 1992年和1993年，KnlJdsen和Biham各自独立地提出了相关密钥攻击。
相关密钥攻击反映了密钥扩展算法对分组密码安全性的影响。
在这种攻击下，攻击者不知道密钥，但他可以选择与当前密钥相关的其他密钥，他可以选择密钥之间的关系，利用分组密码密钥扩展算法的弱点，通过选择合适的、与当前密钥相关的密钥，寻求原有密钥与新的相关密钥下分别对应的加密算法之间的关联，就有可能恢复出密码的密钥。
相关密钥攻击的假设在某些密码应用环境是可以实现的，比如，以分组密码为基础设计的一些MAC算法，分组密码密钥之间的关系是已知的。
相关密钥攻击从一定程度上反映了密钥扩展算法对密码安全性的影响。
一般地，密钥扩展算法将种子密钥扩展成若干子密钥，将各个子密钥嵌入到加密（解密）算法的轮变换中。
相关密钥分析方法在提出之初，仅适用于密钥扩展算法有以下特点的密码：生成子密钥的算法采用了相同的递归表达式。
DES对相关密钥攻击免疫，这是因为在DES密钥扩展算法的递归表达式中，生成一部分子密钥时进行移位为1的操作，而生成其他子密钥时则进行移位为2的操作。
之后大量的研究结果表明：在相关密钥攻击的假设下，结合其他密码分析方法，比如差分密码分析、矩阵攻击、不可能差分密码分析。

<<分组密码的设计与分析>>

编辑推荐

信息安全理论与技术系列丛书　　信息安全国家重点实验室推荐用书　　国家科学技术学术著作出版基金资助项目

<<分组密码的设计与分析>>

版权说明