<<信息保护>>

图书基本信息

书名：<<信息保护>>

13位ISBN编号：9787121068560

10位ISBN编号：7121068567

出版时间：2008-9

出版时间：电子工业出版社

作者：（美）楼坡（Loepp，S.），（美）伍特斯（Wootters，W.） 著；吕欣，马智，许亚杰 译

页数：234

<<信息保护>>

前言

对于许多日常传输任务来说，保护数字信息免受噪声干扰和窃听是非常重要的。
这本介绍纠错编码和密码学的书，用几个重要章节介绍量子密码和量子计算的基础理论，为数学和物理思想的交融提供了一个良好的平台。
本书通过对Shor量子因子分解算法等内容的阐述，将当前量子信息理论的基本观点传递给读者，并启发式地展现了数学与科学问的奇妙关系。
特别有趣的问题是量子物理对密码学带来的潜在影响：①如果能成功制造出一台量子计算机，就能破解我们当前使用的公钥密码系统；②量子密码在未来有望替代这种不能抵抗量子算法攻击的密码体系，这是建立在自然法则基础之上，而非基于计算复杂性理论。
读者即使不懂量子力学，只要具备基本的复数、向量空间和矩阵的知识，都可以读懂本书，并从中受益。
Susan Loepp是威廉姆斯（Williams）大学数学和统计系的一位数学专业副教授。
她的主要研究兴趣是交换代数，特别是基于环上的交换代数。
William K.Wootters是美国物理学会的会员，威廉姆斯大学物理系的自然哲学教授。
他主要研究量子纠缠及量子信息的有关理论。
作者将密码学和编码学这两个热门学科融合在一起，并利用经典与量子等计算和通信模型分别对其进行观察和讨论。
这些引人入胜的内容通过代数结构和相关技巧的逐步展开而有机地结合在一起。
通过学习，学生将会在群、有限域和向量空间的理论及它们的具体应用上，有更为开阔的思路。

<<信息保护>>

内容概要

本书以密码学和量子物理为切入点，深入介绍了量子密码和量子纠错码的主要思想和方法。
针对密码学和编码学，分别从经典信息学和量子信息学两个角度进行了讨论和比较分析，重点介绍了量子密码和量子纠错码的基础理论和研究进展。
主要内容包括：密码学绪论；量子力学；量子密码：纠错码介绍：量子密码的深入探讨；推广的RS码；量子计算等。
本书可以作为计算机、通信、信息安全、密码学、数学、物理学等专业研究生和本科生的教材，也可供从事相关专业的教学、科研人员参考使用。

作者简介

作者：(美国)楼坡 (Susan Loepp) (美国)伍特斯 (William K.Wootters) 译者：吕欣 马智 许亚杰

<<信息保护>>

书籍目录

章节摘录

插图：

<<信息保护>>

编辑推荐

《信息保护:从经典纠错到量子密码》由电子工业出版社出版。

<<信息保护>>

版权说明