# <<信息安全中的数学方法与技术>>

## 图书基本信息

书名：<<信息安全中的数学方法与技术>>

13位ISBN编号：9787302209669

10位ISBN编号：7302209669

出版时间：2009-10

出版时间：清华大学出版社

作者：冯登国

页数：437

## 前言

信息安全作为一门重要的学科方向，与其他学科一样，有其自身的方法论。
从理论与技术研究角度来看，信息安全有其自身的研究方法学；从管理角度来看，信息安全有其自身的管理方法学；从工程与应用角度来看，信息安全有其自身的工程方法学。
本书重点讲述信息安全的研究方法学，我们称之为信息安全中的数学方法与技术。
数学方法与技术是研究和掌握信息安全理论与技术的基础和工具。
面向信息安全专业本科生教育的数学教材《信息安全数学基础》是从基础的角度介绍与信息安全相关的数学基础知识，本书则是从研究与打基础并重的角度介绍研究和掌握信息安全理论与技术必备的数学方法与技术。
本书的特点如下：（1）内容全面。
涵盖了当前研究信息安全理论与技术的主要方法与技术，包括初等数论、代数、椭圆曲线、组合论、图论、概率论、信息论、数理统计、随机过程、频谱、纠错编码、计算复杂性、数理逻辑、数字信号处理、数据挖掘、软件安全性分析等方法与技术。
（2）针对性强。
紧密结合信息安全理论与技术研究的需求和掌握信息安全理论与技术工具的需求，重点介绍研究方法与技术，并选择有代表性的应用进行举例，将研究方法与技术和信息安全融为一体。
不仅适用于专门从事信息安全研究的专业人员，而且也适用于从事相关理论与技术的研究人员了解理论与技术在信息安全中的应用示范。
（3）起点高。
重点从研究的视角介绍信息安全中的数学方法与技术，并对方法和技术做了高度提炼。
例如，纠错编码方法与技术这一章，不仅是对信息安全研究中所用到的纠错编码方法与技术的高度总结，而且也是现有纠错编码重要方法与技术的一个高度概括。

## 内容概要

本书主要介绍了研究和掌握信息安全理论与技术必备的数学方法与技术，主要内容包括初等数论、代数、椭圆曲线、组合论、图论、概率论、信息论、数理统计、随机过程、频谱、纠错编码、计算复杂性、数理逻辑、数字信号处理、数据挖掘等方法与技术，并同步介绍了这些方法与技术在信息安全中的典型应用。

本书可作为高等院校信息安全、密码学、数学、计算机、通信等专业的博士生、硕士生和本科生的教科书，也可供从事相关专业的教学、科研和工程技术人员参考。

# <<信息安全中的数学方法与技术>>

## 书籍目录

## 章节摘录

插图：15.3.4 聚类聚类也称为簇（cluster），是指一个数据对象的集合。
其特点是在同一个类中的对象之间具有相似性，而在不同类的对象之间是相异的。
聚类分析就是把一个给定的数据对象集合分成不同的簇的过程。
聚类是一种无监督分类法，没有预先指定的类别。
其典型的应用是作为一个独立的分析工具，用于了解数据的分布，或作为其他算法的一个数据预处理步骤。
聚类分析在市场销售、土地使用、保险、城市规划、地震研究等各个领域获得了广泛的应用。
一个好的聚类方法要能产生高质量的聚类结果一一簇。
这些簇要具备两个特点，即高的簇内相似性和低的簇间相似性。
聚类结果的好坏取决于该聚类方法采用的相似性评估方法以及该方法的具体实现，聚类结果的好坏还取决于该聚类方法是能发现某些还是所有的隐含模式。
通常来说，聚类算法需要满足以下特性：·可伸缩性；·能够处理不同类型的属性；·能发现任意形状的簇；·在决定输入参数时，尽量不需要特定的领域知识；·能够处理噪声和异常；·对输入数据对象的顺序不敏感；·能处理高维数据；·能产生一个好的、能满足用户指定约束的聚类结果；·结果是可解释的、可理解的和可用的。
对于聚类算法而言，如何衡量两个对象之间的相似度（相异度）是至关重要的。
通常使用距离来进行衡量。
对不同类型的变量，距离函数的定义通常是不同的，而且，根据实际的应用和数据的语义，在计算距离时，不同的变量有不同的权值相联系。
常用的距离度量方法如下。

## 编辑推荐

《信息安全中的数学方法与技术》：信息安全国家重点实验室推荐用书，国家重点基础研究发展规划项目资助（项目编号：2007CB311202），国家自然科学基金重点项目资助（项目编号：60833008）。

## 版权说明