<<消息认证码>>

图书基本信息

书名：<<消息认证码>>

13位ISBN编号：9787312022272

10位ISBN编号：7312022278

出版时间：2009-5

出版时间：中国科学技术大学出版社

作者：裴定一

页数：268

前言

大学最重要的功能是向社会输送人才。
大学对于一个国家、民族乃至世界的重要性和贡献度，很大程度上是通过毕业生在社会各领域所取得的成就来体现的。
中国科学技术大学建校只有短短的50年，之所以迅速成为享有较高国际声誉的著名大学之一，主要就是因为她培养出了一大批德才兼备的优秀毕业生。
他们志向高远、基础扎实、综合素质高、创新能力强，在国内外科技、经济、教育等领域做出了杰出的贡献，为中国科大赢得了“科技英才的摇篮”的美誉。
2008年9月，胡锦涛总书记为中国科大建校五十周年发来贺信，信中称赞说：半个世纪以来，中国科学技术大学依托中国科学院，按照全院办校、所系结合的方针，弘扬红专并进、理实交融的校风，努力推进教学和科研工作的改革创新，为党和国家培养了一大批科技人才，取得了一系列具有世界先进水平的原创性科技成果，为推动我国科教事业发展和社会主义现代化建设做出了重要贡献。
据统计，中国科大迄今已毕业的5万人中，已有42人当选中国科学院和中国工程院院士，是同期（自1963年以来）毕业生中当选院士数最多的高校之一。
其中，本科毕业生中平均每1000人就产生工名院士和700多名硕士、博士，比例位居全国高校之首。
还有众多的中青年才俊成为我国科技、企业、教育等领域的领军人物和骨干。
在历年评选的“中国青年五四奖章”获得者中，作为科技界、科技创新型企业界青年才俊代表，科大毕业生已连续多年榜上有名，获奖总人数位居全国高校前列。

<<消息认证码>>

内容概要

保密和认证是信息安全的两个重要方面。
信息的认证用于鉴别信息的真伪，认证方法有无条件安全和计算安全两种类型。
本书主要研究无条件安全的认证理论，介绍了作者在这个领域的研究成果。
首先分别引入了三方（发方、收方和敌方）及四方（发方、收方、敌方和仲裁方）认证系统的完善认证概念，然后用组合设计的语言刻画了这两类完善认证码的结构，在此基础上找到了完善认证码的构造方法。
书中介绍了作者利用有理正规曲线构造的一类三方完善认证码，同时也介绍了其他构造完善认证码的方法，例如基于t设计、基于单位指标正交阵列和基于有限几何的构造方法。
本书最后两章研究具有保密功能的认证码的性质和构造方法，附录中简要介绍了基于Hash函数的消息认证码。
　本书可供学习密码学的大学生、研究生作为教学参考书，也可供数学类专业学生和密码学研究人员参考。

<<消息认证码>>

书籍目录

章节摘录

插图：第2章 认证系统保密和认证是信息安全的两个重要方面。
保密是为了防止机密信息被非授权接触的人窃取；认证是为了确认信息来源方的身份，以及发现信息在传输、存储过程中是否被篡改，换句话说，认证是为了鉴别假冒别人身份发送的伪造信息.保密和认证是两个互相独立的概念.在一个信息系统中，可以只考虑保密不考虑认证，也可以只考虑认证不考虑保密，也可以两者同时考虑.2.1 三方认证模型（A－码）认证系统是从现实的认证问题中抽象出来的一个认证模型.假定在一个认证模型中包含三方：发方、收方和敌方，发方要向收方发送信息，敌方想假冒发方向收方发送虚假信息，或者想篡改发方的信息，以达到欺骗收方的目的.因此发方和收方必须设法防止来自敌方的欺骗.在三方认证模型中，假定发方和收方是互相信任的，他们不会互相欺骗.当发方和收方也可能互相欺骗时，就需要在认证模型中增添仲裁方.发方打算给收方传递的消息称为信源，以y表示所有信源的集合。
为了防止敌方的欺骗，发方将信源按照一个编码规则进行编码变换后再发送。

编辑推荐

《消息认证码》是裴定一编著的，由中国科学技术大学出版社出版。

<<消息认证码>>

版权说明