消息认证码

作者：裴定一著

出版社：中国科技大学出版社

出版日期：2009.05

总页数：268

介绍：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。