

密码协议基础

[密码协议基础_下载链接1](#)

著者:

出版者:

出版时间:2009-1

装帧:

isbn:9787040251548

《密码协议基础》较为全面、深入地介绍了信息安全体系中的基础密码协议、高级密码协议及应用密码协议，按照由浅入深的原则，将全书分为13章，内容包括三大部分：基础密码协议、高级密码协议及应用密码协议。基础密码协议由引论、密钥协商、实体认证、比特承诺协议组成；高级密码协议部分包括高级签名协议、零知识、不经意传输、秘密分享和门限密码、安全多方计算协议；应用密码协议部分包括Kerberos协议、IKE密钥管理协议、电子现金及无线安全通信。《密码协议基础》对各类密码协议及其相关应用进行了详细的论述和分析，可作为高校计算机、信息安全、电子信息与通信、信息与计算科学等专业高年级本科生和研究生的教学参考书，也可作为相关工程技术人员学习信息安全知识的入门读物。通过阅读《密码协议基础》，读者不仅能够全面熟悉和了解各类密码协议的设计理念和机制，还可以提高密码及相关安全协议的独立设计和分析能力。

作者介绍:

目录:

[密码协议基础_下载链接1](#)

标签

密码

信息安全

评论

[密码协议基础_下载链接1](#)

书评

[密码协议基础_下载链接1](#)