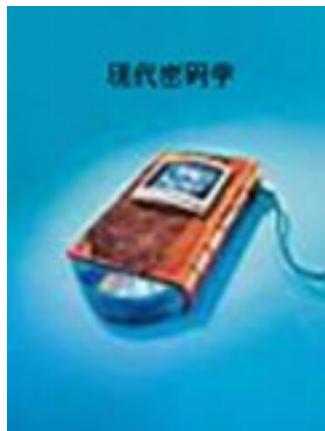


# 现代密码学



[现代密码学\\_下载链接1](#)

著者:

出版者:

出版时间:2009-2

装帧:

isbn:9787030236357

《现代密码学:理论、方法与研究前沿》是一本现代密码学的入门书，书中系统地讲解了现代密码学研究所需要的预备知识、基础理论与研究中使用的理论工具、证明方法、协议构造方法，以及现代密码学研究的若干前沿领域。《现代密码学:理论、方法与研究前沿》分10章，内容包括预备知识、理论计算机科学基础、数论与代数基础、传统密码学协议的设计与分析、单向散列函数与随机性、公开密钥算法与数字签名、数字承诺、零知识证明与不经意传输、多方保密计算、量子密码学等。

《现代密码学:理论、方法与研究前沿》可作为数学、计算机科学与技术、信息安全、通信等专业科研人员的参考书，也可供相关的教师、研究生参考。

作者介绍:

目录:

[现代密码学 下载链接1](#)

标签

数学

评论

这是一本大杂烩么？

---

[现代密码学 下载链接1](#)

书评

---

[现代密码学 下载链接1](#)