公钥密码学

公钥密码学_下载链接1_

著者:祝跃飞

出版者:高等教育出版社

出版时间:2010-1

装帧:

isbn:9787040285024

《公钥密码学:设计原理与可证安全》重点介绍公钥密码的可证安全理论和旁道攻击技术，内容包括公钥密码基础理论、公钥密码的可证安全理论和旁道攻击三个部分。第一部分为公钥密码学基础理论，介绍了公钥密码体制的提出和特点、公钥密码与杂凑函数、公钥基础设施以及基本体制；第二部分为公钥密码体制的可证安全理论，重点论述加密体制的可证安全、签名体制的可证安全以及混合加密体制的可证安全性分析；第三部分概略介绍公钥密码的旁道攻击技术。

《公钥密码学:设计原理与可证安全》适合高等学校计算机、信息安全、电子信息与通信、信息与计算科学等专业的研究生以及相关专业的研究人员使用。

作者介绍:

目录:

标签

评论

公钥密码学_下载链接1_

书评

公钥密码学_下载链接1_